Notation and number systems:
Set of integers = \{ \ldots , -3, -2, -1, 0, 1, 2, \ldots \} = \mathbb{Z}.
Set of rational numbers = \{ \frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0 \} = \mathbb{Q}. (\mid \text{ is "such that", not divides}).
Set of real numbers = \{ \text{decimals} \} = \mathbb{R}, \text{ includes } \sqrt{2}, -\pi, e.

Irrational means \( \mathbb{R} \setminus \mathbb{Q} \) (real but not rational).

Imprecise: If \( m \) is a multiple of \( b \) then we say \( b \) divides \( m \).

Precise: Let \( b \in \mathbb{Z}_{\neq 0} \) and \( m \in \mathbb{Z} \). If there's a \( c \in \mathbb{Z} \) with \( m = bc \) then we say \( b \) \textbf{divides} \( m \) and write \( b \mid m \). We say \( b \) is a divisor of \( m \).

Ex 1. 3|12, 7| - 7 (since \(-7 = 7 \cdot -1\)), 8|0 (since \( 0 = 8 \cdot 0 \)).

If no such \( c \) exists we say \( b \) doesn't divide \( m \) and write \( b \nmid m \).

Prop 2. If \( a, b \in \mathbb{Z} \) and \( a \mid b \) and \( b \neq 0 \) then \( |a| \leq |b| \).

Pf. We have \( b = ma \) for some \( m \in \mathbb{Z} \). Since \( b \neq 0 \) we have \( m \neq 0 \). We have \( |b| = |ma| = |m||a| \) and \( m \in \mathbb{Z}_{\neq 0} \Rightarrow 1 \leq |m| \). So \( |a| \leq |a||m| = |b| \). End pf.

If \( p \in \mathbb{Z}_{\geq 2} \) and the only positive divisors of \( p \) are 1 and itself (\( p \)) then call \( p \) a \textbf{prime} number.

If \( n \in \mathbb{Z}_{\geq 2} \) isn't prime it's \underline{composite}. 1 is neither prime nor composite.

((Ed, prepare this Theorem and proof))

Theorem 3. If \( n \in \mathbb{Z}_{\geq 2} \) then \( n \) is a prime or it can be represented as a product of primes.

Principle of strong mathematical induction. Assume that a set contains 1. Assume also that if the set contains the integers 1, 2, 3, …, \( k \) then \( k+1 \) is also the set. Then the set contains all positive integers.

How to use for a proof by induction. You want to prove that a statement is true for all positive integers \( n \). So you want to show that the set of integers for which the statement is true contains 1 (i.e. the statement is true for \( n = 1 \)). Next you want to show that whenever the set of integers for which the statement is true contains 1, …, \( k \), for some \( k \) then it also contains \( k+1 \) (i.e. if the statement is true for 1, …, \( k \) then it is true for \( k+1 \)). This implies that the set of integers for which the statement is true contains all positive integers (i.e. the statement is true for all positive integers).

For this proof, start at \( n = 2 \), not \( n = 1 \).

Proof. ((First show statement is true for first \( n = 2 \)). The statement is true for \( n = 2 \) since 2 is prime. Assume the statement holds for all integers 2, …, \( k \) for some \( k \geq 2 \). ((Now show statement true for \( k+1 \)). If \( k+1 \) is prime, then we're done. If \( k+1 \) is not prime then it has some divisor \( b \) with \( 1 < b < k+1 \) (Prop 2 gives 2nd <). Let \( c = \frac{k+1}{b} \). We know \( c \in \mathbb{Z} \). Since \( b > 1 \), we have \( c = \frac{k+1}{b} < k+1 \). Since \( b < k+1 \), we have \( 1 < \frac{k+1}{b} = c \). Thus \( 1 < c < k+1 \) also. Since \( 2 \leq b \leq k \) and \( 2 \leq c \leq k \), we can write \( b \) and \( c \) as primes or products of primes by the assumption. So \( k+1 = bc \) can be written as a product of primes. By the principle of strong induction, the statement holds for all \( n \in \mathbb{Z}_{\geq 2} \). End pf.

To here, first lecture

Prop 4. Let \( a, b, c, x, y \in \mathbb{Z} \).
   i) \( a|b \) and \( b|c \Rightarrow a|c \).
   ii) \( a|b \) and \( a|c \Rightarrow a|b+c \).
   iii) \( a|b \) and \( a|c \Rightarrow a|bx + cy \).
   iv) Assume \( x \neq 0 \). Then \( a|b \) iff \( xa|xb \).

Proof. i) \( \exists m, n \in \mathbb{Z} \text{ s.t. } b = ma, c = nb \). Thus \( c = nma \) so \( a|c \).
ii) \( \exists m, n \in \mathbb{Z} \) s.t. \( b = ma, c = na \). Thus \( b + c = ma + na = (m + n)a \) so \( a|b + c \).

iii) \( \exists m, n \in \mathbb{Z} \) s.t. \( b = ma, c = na \). Thus \( bx + cy = max + nay = (mx + ny)a \) so \( a|bx + cy \).

iv). ((Must show \( \Rightarrow \) and \( \Leftarrow \)) If \( a|b \) then \( \exists m \in \mathbb{Z} \) s.t. \( b = ma \). So \( xb = m(xa) \) and \( xa|xb \). If \( xa|xb \) then \( \exists n \in \mathbb{Z} \) s.t. \( xb = nxa \). Since \( x \neq 0 \) we have \( b = na \) so \( a|b \). End pf.

Cor 5. If \( a, b \in \mathbb{Z}_{>0} \) and if \( a|b \) and \( b|a \) then \( a = b \).

Pf. Since \( a|b \) we have \( a = |a| \leq |b| = b \). Similarly \( b|a \Rightarrow b \leq a \). Thus \( a = b \). End pf.

Ex 6. For each \( n \in \mathbb{Z}_{\geq 1} \) we have \( 5|2^{4n+2} + 1 \).

Principle of (weak) mathematical induction. Assume that a set contains 1. In addition, whenever the set contains \( k \) it also contains \( k + 1 \). Then the set contains all positive integers.

Proof. The statement holds for \( n = 1 \) since \( 2^{4+2} + 1 = 65 = 5 \cdot 13 \). Assume statement holds for some one fixed \( k \in \mathbb{Z}_{\geq 1} \). (What does that give us?) Thus \( 2^{4k+2} + 1 = 5c \) for some \( c \in \mathbb{Z} \). (Now need to show that \( 5|2^{4(k+1)+2} + 1 \)).

We have \( 2^{4(k+1)+2} + 1 = 2^{4k+6} + 1 \). (We Know something about \( 2^{4k+2} + 1 \)) Now \( 2^{4k+6} + 1 = 2^{4k+2}16 + 1 = (5c - 1)16 + 1 = 5 \cdot 16c - 15 = 5(16c - 3) \). So \( 5|2^{4(k+1)+2} + 1 \).

So the statement holds for \( k + 1 \). So by the principle of mathematical induction, the the statement holds for all \( n \in \mathbb{Z}_{\geq 1} \).

End pf.

Well-ordering principle: Every non-empty set of positive integers contains a least element.

Note: could replace “positive integers” by “integers \( \geq n \)” for any \( n \in \mathbb{Z} \).

Read Thm 1.4 and proof on page 21. (\( \sqrt{2} \) is irrational).

Thm 7. Let \( d \in \mathbb{Z} \) and \( b \in \mathbb{Z}_{>1} \). There are unique integers \( q \) and \( r \) with \( 0 \leq r < b \) such that \( d = qb + r \).

Note: \( b \) is divisor, \( q \) is quotient, \( r \) is remainder, \( (d \) is dividend).

Ex 8. \( d = 96, b = 7, 96 = 13 \cdot 7 + 5 \) so \( q = 12, r = 5 \).

Pf. Consider the set \( \{d - nb \mid n \in \mathbb{Z}, d - nb \geq 0\} \). Aside \( \{\ldots 96, 89, 82, 75, \ldots, 19, 12, 5\} \) End Aside. It’s a subset of \( \mathbb{Z}_{\geq 0} \), so by well-ord prin it has a smallest element \( d - qb \), which we all call \( r \). So \( d - qb = r \) and \( d = qb + r \).

((Show \( 0 \leq r < b \)) We’ve assumed \( r \) in set so \( r \geq 0 \). If \( r \geq b \) then \( d - q'b \geq b \) so \( d - (q + 1)b \geq 0 \), contradicting fact that \( r \) is least such element. So \( 0 \leq r < b \). ((Show \( q, r \) unique)) Say \( d = qb + r = q'b + r' \) with \( 0 \leq r' < b \). Then \( (q - q')b = r' - r \). Since \( 0 \leq r < b, 0 \leq r' < b \) we have \( -b < r' - r < b \) and \( b|r' - r \). So \( r' - r = 0 \) and \( r' = r \). Note \( q = \frac{d - r}{b} \) and \( q' = \frac{d - r'}{b} = \frac{d - r}{b} = q \). So \( r \) and \( q \) are indeed unique.

To here, second lecture

Prop 9. If \( n \in \mathbb{Z} \) and divide \( n^2 \) by 4 then the remainder is 0 or 1.

Proof. From Thm 7, \( n = 4q + r \) with \( q \in \mathbb{Z} \) and \( 0 \leq r < 4 \) so \( r = 0, 1, 2, 3 \).

Case 1. \( n = 4q + 0 \). Then \( n^2 = 16q^2 = 4(4q^2) + 0 \) so the remainder is 0.

Case 2. \( n = 4q + 1 \). Then \( n^2 = 16q^2 + 8q + 1 = 4(4q^2 + 2q) + 1 \) so the remainder is 1.

Case 3. \( n = 4q + 2 \). Then \( n^2 = 16q^2 + 16q + 4 = 4(4q^2 + 4q + 1) + 0 \) so the remainder is 0.

Case 4. \( n = 4q + 3 \). Then \( n^2 = 16q^2 + 24q + 9 = 4(4q^2 + 6q + 2) + 1 \) so the remainder is 1. End Pf.

Let \( a, b \in \mathbb{Z} \) and not both 0. The greatest common divisor of \( a \) and \( b \) is denoted \( \text{gcd}(a, b) \) or \( (a, b) \). Since 1 is always a common divisor, the \( \text{gcd} \) is positive.
Ex 10. What’s (24, 36)? Compare $\frac{24}{36}$.

What’s (25, 36), (10, 36), (−5, 0), (1, 18), (8, −8)?
Thm 11. Let $a, b \in \mathbb{Z}$ and not both 0 and $g = (a,b)$. Then $g$ is the least element of $S_{a,b} = \{ax + by \mid x, y \in \mathbb{Z}, ax + by > 0\}$.

Ex 12. $a = 4, b = 18$. Set $S_{4,18}$ contains $5 \cdot 4 + (-1) \cdot 18 = 2, 1 \cdot 4 + 0 \cdot 18 = 4, -3 \cdot 4 + 1 \cdot 18 = 6$, etc.

Pf. The set $S_{a,b}$ has a least element $l$ from well-ordering principle. So $l = ax_0 + by_0$ for some $x_0, y_0 \in \mathbb{Z}$.

Ex 15. $(10, 20, 25) = 5$.

Ex 16. Find $(600, 252)$. Method 1. $600 = 2^3 \cdot 3^1 \cdot 5^2, 252 = 2^2 \cdot 3^2 \cdot 7^1$. So $(600, 252) = 2^2 \cdot 3 = 12$. End ex.

Cor 13. If $d|a$ and $d|b$ then $? d|(a,b)$.

In words: Common divisors divide the gcd.

Prop 14. If $a, b \in \mathbb{Z}$, not both 0, and $g = (a,b)$ then $(a_g, b_g) = ? 1$.

Ex 17. Find $(600, 252)$. Method 2. If $a > b > 0$, start $a = qb + r \ldots$

Let $a, b \in \mathbb{Z}$ with $a > b > 0$. The Euclidean algorithm to find $(a,b)$.
Write \[ a = q_1 b + r_1 \quad 0 \leq r_1 < b \]
\[ b = q_2 r_1 + r_2 \quad 0 \leq r_2 < r_1 \]
\[ r_1 = q_3 r_2 + r_3 \quad 0 \leq r_3 < r_2 \]
\[ \vdots \]
\[ r_{n-3} = q_{n-1} r_{n-2} + r_{n-1} \]
\[ r_{n-2} = q_n r_{n-1} + r_n \]
\[ r_{n-1} = q_{n+1} r_n + (r_{n+1} = 0) \]

Since \( r_1 > r_2 > r_3 > \ldots \geq 0 \), process must terminate with some \( r_{n+1} = 0 \). Turns out \( r_n = (a, b) \).

To here, third lecture

Sketch of pf that \( r_n = (a, b) \). First show \( r_n|(a, b): r_n|r_{n-1} \) so \( r_n|q_nr_{n-1} + r_n = r_{n-2} \) from Prop 4iii. And \( r_n|q_{n-1}r_{n-2} + r_{n-1} = r_{n-3} \), \ldots, \( r_n|b \), \( r_n|a \) so \( r_n|(a, b) \) by Cor 13.

Let \( g = (a, b) \). Show \( g|r_n; g|a, g|b \) so \( g|a - q_1 b = r_1 \). And \( g|b - q_2 r_1 = r_2 \), \( g|r_1 - q_3 r_2 = r_3 \), \ldots, so \( g|r_n \).

Since \( r_n|(a, b) \) and \( g = (a, b) \) and both positive have \( r_n = (a, b) \). End sketch.

Thm 11 implies that 12 is least element of \( \{ 252x + 600y \mid x, y \in \mathbb{Z}, 252x + 600y > 0 \} \).

Working backwards through Eucl alg’m gives us one such pair \( x, y \).

\[
12 = (36) - 1(24) \quad \text{repl smaller}
\]
\[
= (36) - 1(60 - 36) \quad \text{simplify}
\]
\[
= 2(36) - 1(60) \quad \text{repl smaller}
\]
\[
= 2(36) - 1(60 - 36) \quad \text{simplify}
\]
\[
= 2(96 - 3(60)) \quad \text{repl smaller}
\]
\[
= 2(96 - 3(252) - 2 \cdot 96) \quad \text{simplify}
\]
\[
= 2(600 - 2 \cdot 252) - 3(252) \quad \text{repl smaller}
\]
\[
= 8(600) - 19(252) = 12
\]

Thm 18. If \( a|bc \) and \( (a, b) = 1 \) then ?? \( a|c \).

Pf. From Thm 11 \( \exists x, y \in \mathbb{Z} \) s.t. \( ax + by = 1 \). Thus \( cax + bey = c \). Since \( a|bc \) and \( a|cax \) then \( a|c \). End pf.

Cor 19. If \( p \) is prime and \( p|bc \) then \( p|b \) or \( p|c \).

Note: Some use this as the definition of prime.

Pf. If \( p|b \) we’re done. Assume \( p \not| b \). We know \( (b, p) \) is a positive divisor of \( p \), which isn’t \( p \), so it’s 1. From Thm 18, \( p|c \). End pf.

Ex 19.5 If \( 5|c \) and \( 6|c \) then ? If \( 4|c \) and \( 6|c \) then ?

Thm 20. If \( a|c \) and \( b|c \) and \( (a, b) = 1 \) then \? \( ab|c \).

Pf. \( \exists m \in \mathbb{Z} \) s.t. \( ma = c \). Thus \( b|ma \). Since \( (a, b) = 1 \) we have \( b|m \) from Thm 18. So \( ab|am = c \).

The least common multiple of \( a, b \in \mathbb{Z}_{\neq 0} \) is the smallest positive integer that \( a \) and \( b \) both divide. It is denoted \([a, b]\).

Prop’n 21. Let \( a, b \in \mathbb{Z}_{\neq 0} \). Then \([a, b]\) divides any common multiple of \( a \) and \( b \).
Pf. Let \( m \) be a common multiple of \( a \) and \( b \). Can write \( m = q[a, b] + r \) where \( 0 \leq r < [a, b] \). Since \( a|m \) and \( a[q[a, b]] \) we have \( a|(m - q[a, b]) = r \). Similarly \( b|r \). So \( r \) is a common multiple, but it's not the LCM so it's not positive. So \( r = 0 \) and \( [a, b]|m \). End pf.

To here, fourth lecture.

Want to connect \([a, b]\) and \((a, b)\). ((Need some technical lemmas first..)) When is \([a, b]\) obvious? When \((a, b) = 1\).

Lemma 22. Let \( a, b \in \mathbb{Z}_{\geq 1} \). If \((a, b) = 1\) then \([a, b] = ab\).

Pf. Let \( g = \frac{a}{c} \) and \( m = [a, b] \). Make much use of \( ab \) iff \( xa|xb \) when \( x \neq 0 \). End aside. Have \( \frac{a}{g} m \) and \( \frac{b}{g} c \) so \( [a, c]j \) and \( b|c \). From Prop 21, \((a, b)\) any common mult)) \( m|j \) and \( m|b \). Since \( a|m \) and \( b|m \) we know \( \frac{a}{m} m \) and \( \frac{b}{c} c \) so \( j \frac{m}{c} \). Thus \( j = \frac{m}{c} \). End pf.

Lemma 23. Let \( a, b, c \in \mathbb{Z}_{\geq 1} \). If \( c|a \) and \( c|b \) then \( \frac{a}{c}, \frac{b}{c} = \frac{[a, b]}{c} \).

Pf. Let \( g = (a, b) \). From Lemma 22, \( \frac{a}{g}, \frac{b}{g} = \frac{[a, b]}{g} \). From Prop 14, \((a, b), (a, c) = 1 \) and so from Lemma 23 \( \frac{a}{g}, \frac{b}{g} = \frac{a}{g}, \frac{b}{g} \). Thus \( [a, b] = \frac{ab}{g} \). End pf.

Thm 24. Let \( a, b \in \mathbb{Z}_{\geq 1} \). Then \( [a, b] = \frac{ab}{(a, b)} \).

Pf. Let \( g = (a, b) \). From Lemma 22, \( \frac{a}{g}, \frac{b}{g} = \frac{[a, b]}{g} \). From Prop 14, \((a, b), (a, c) = 1 \) and so from Lemma 23 \( \frac{a}{g}, \frac{b}{g} = \frac{[a, b]}{g} \). Thus \( [a, b] = \frac{ab}{g} \). End pf.

Thm 25. If \( a_1, \ldots, a_r \in \mathbb{Z}_{\neq 0} \) then \((a_1, a_2, \ldots, a_r) = ((a_1, \ldots, a_{r-1}), a_r) \) and \([a_1, \ldots, a_r] = [[a_1, \ldots, a_{r-1}], a_r] \).

Won't prove.

Ex 26. Find \([299, 221, 161]\). That's \([299, 221, 161]\). Now \([299, 221] = \frac{299 \cdot 221}{(299, 221)} = 299 \cdot 221 = 83 \cdot 7 \cdot 11 \cdot 13 \cdot 78 \cdot 1 \cdot 65 + 13, 65 = 5 \cdot 13 + 0 \). So \([299, 221] = 13 \cdot 13 \cdot 299, 221\) = \(\frac{299 \cdot 221}{13} = \frac{5083}{13} = 5083 \). Thus \([299, 221, 161] = [5083, 161] = \frac{5083 \cdot 161}{(5083, 161)} \). 5083 = 1 \cdot 69 + 23, 69 = 3 \cdot 23 + 0 \). So \([5083, 161] = 23 \cdot 23 \cdot 5083, 161\) = \(\frac{5083 \cdot 161}{23} = 35581 = [299, 221, 161] \). We'll prove soon that factorization of positive integers into product of primes is unique. This is actually special.

Let \( \mathbb{Z}[\sqrt{-6}] = \{a + b\sqrt{-6} \mid a, b \in \mathbb{Z}\} \). Much like \( \mathbb{Z} \). Commut group under add'n. Mult'n is closed \((a + b\sqrt{-6})(c + d\sqrt{-6}) = (ac - 6bd) + (ad + bc)\sqrt{-6} \), commutative and assoc. Distrib laws.

To here, fifth lecture.

Let \( x \in \mathbb{Z}[\sqrt{-6}] \), \( x \neq 0, \pm 1 \). Say \( x \) is irreducible if \( \pm 1, \pm x \) are its only divisors.

Can use norm to show irreducibility.

Let \( \mathbb{N} : \mathbb{Z}[\sqrt{-6}] \to \mathbb{Z} \) by \( N(a + b\sqrt{-6}) = a^2 + 6b^2 \).

Prop 27. i) \( x \in \mathbb{Z}[\sqrt{-6}] \Rightarrow N(x) \geq 0 \).
ii) \( N(x) = 0 \iff x = 0 \).
iii) \( N(x) = 1 \iff x = \pm 1 \).
iv) $x \in \mathbb{Z} \Rightarrow N(x) \text{ is a square in } \mathbb{Z}$.

v) If $x \not\in \mathbb{Z}$ then $N(x) \geq 6$. ((Note $b \neq 0$))

vi) $x, y \in \mathbb{Z}[\sqrt{-6}] \Rightarrow N(xy) = N(x)N(y)$. (homework) End Prop.

Prop 28. 5 is irreducible in $\mathbb{Z}[\sqrt{-6}]$.

Proof. Say $x, y \in \mathbb{Z}[\sqrt{-6}]$ and $xy = 5$. Then $25 = N(5) = N(xy) = N(x)N(y)$. So $\{N(x), N(y)\} = \{1, 25\}$ or $\{5, 5\}$.
Case 1: $N(x) = N(y) = 5$. From v), $x, y \in \mathbb{Z}$, but from iv), impossible.
Case 2: $\{N(x), N(y)\} = \{1, 25\}$. Without loss of generality (WLOG) let $N(x) = 1$. From Prop 27, iii) have $x = \pm 1, y = \frac{5}{2} = \pm 5$. So $x, y \in \{\pm 1, \pm 5\}$. End pf.

Similarly can show 2, 2 + $\sqrt{-6}, 2 - \sqrt{-6}$ are irreducible in $\mathbb{Z}[\sqrt{-6}]$. Note $10 = 2 \cdot 5 = (2 + \sqrt{-6})(2 - \sqrt{-6})$ in $\mathbb{Z}[\sqrt{-6}]$, so don’t have unique factorization into irreducibles.

Let $\alpha \in \mathbb{Z}[\sqrt{-6}]$. Say $\alpha$ is prime in $\mathbb{Z}[\sqrt{-6}]$ iff $\forall \beta, \gamma \in \mathbb{Z}[\sqrt{-6}]$ with $\alpha|\beta\gamma$ we have $\alpha|\beta$ or $\alpha|\gamma$.
In $\mathbb{Z}[\sqrt{-6}] \{\text{ primes}\} \neq \{\text{ irre'ds}\}$. For ex: 5 is irred but not prime. Note 5|10 = $(2 + \sqrt{-6})(2 - \sqrt{-6})$, but 5∤(2 + $\sqrt{-6})$ (since $\frac{2}{5} + \frac{\sqrt{-6}}{5} \not\in \mathbb{Z}[\sqrt{-6}]$ and 5∤(2 - $\sqrt{-6}$).

Find irred in $\mathbb{Z}$, that’s red’ble in $\mathbb{Z}[\sqrt{-6}], 7 = (1 + \sqrt{-6})(1 - \sqrt{-6}), 31, p \equiv 1, 5, 7, 11{\text{mod} 24}$.

Rarely true that have unique factoriz into irreds in $\mathbb{Z}[\sqrt{a}]$. Do have it in $\mathbb{Z}[\sqrt{1}]$.

Fundamental Theorem of Arithmetic: Let $n \in \mathbb{Z}_{\geq 2}$. Then $n$ can be written as a product of primes and that product is unique up to order.

Pf. Already proved $n$ can be written as product of primes (used irreducibility criterion). Let $n = p_1\cdots p_r = q_1q_2\cdots q_s$. Write so $p_1 \leq p_2 \leq \ldots$ and $q_1 \leq q_2 \leq \ldots$ and WLOG $r \leq s$.

Now $p_1|n$ so $p_1|q_1q_2\cdots q_s$. From Cor 19, $p_1$ divides one of the $q_i$’s. So $p_1$ is one of the $q_i$’s. Similarly $q_1$ is one of the $p_i$’s. Now $p_1 \leq p_j = q_1 \leq q_i = p_1$, so all same and $p_1 = q_1$. We can cancel and get either 1 = 1, or $1 = q_2\cdots q_2$ (imposs) or $p_2p_3\cdots p_r = q_2q_3\cdots q_s$. We can do this up to $p_r$ and we’ll have 1 = $q_{r+1}\cdots q_s$ (imposs) or 1 = 1. So $r = s$ and $p_1 = q_1, p_2 = q_2, \ldots, p_r = q_r$. End pf.

If $n \in \mathbb{Z}_{\geq 2}$ then can write $n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$ with $p_1 < p_2 < \ldots < p_r$ and $\alpha_i \in \mathbb{Z}_{\geq 1}$. This is called the canonical representation of $n$ as a product of powers of primes.

Thm 29. Let $a = \prod_{i=1}^{r}p_i^{\alpha_i}$ be the canon repr’n of $a \in \mathbb{Z}_{\geq 2}$ and $b \in \mathbb{Z}_{\geq 1}$. Then $b|a \Leftrightarrow b = \prod_{i=1}^{r}p_i^{\beta_i}$ with $0 \leq \beta_i \leq \alpha_i$ for all $i$.

Pf in bk.

Ex. 30.
3240 = $2^3 \cdot 3^4 \cdot 5$.
48114 = $2^1 \cdot 3^3 \cdot 11$. Find (3240, 48114), [3240, 48114].

Thm 31. If $a = \prod_{i=1}^{r}p_i^{\alpha_i}$ and $b = \prod_{i=1}^{r}p_i^{\beta_i}$ with $p_i$’s different and $\alpha_i, \beta_i \geq 0$ then $(a, b) = \prod_{i=1}^{r}p_i^{\min(\alpha_i, \beta_i)}$ and $[a, b] = \prod_{i=1}^{r}p_i^{\max(\alpha_i, \beta_i)}$.

Won’t prove.
To here, sixth lecture.

Ex 32. What are positive divisors of 90?
1 1 1
2 3 5
9

There’s a divisor for each left-to-right path. 1, 5, 3, 15, 9, 45, 2, 10, 6, 30, 18, 90. So 2 · 3 · 2 of them. End ex.

Ex 33. How many positive divisors of 144 = 2^4 · 3^2? From Thm 29, of form 2^a · 3^b with 0 ≤ a ≤ 4, 0 ≤ b ≤ 2 so 5 · 3 = 15. End ex.

Let τ(n) be the number of positive divisors of n. If n = p_1^{a_1}p_2^{a_2} · · · p_r^{a_r} = ∏_{i=1}^r p_i^{a_i} (canon rep’n) then τ(n) = ∏_{i=1}^r (a_i + 1).

The sum of the positive divisors of n is denoted σ(n). (Studied by Pythagoreans.)

Ex 34. σ(144) = (1 + 2 + 4 + 8 + 16) ((from 2’s)) + (3 + 6 + 12 + 24 + 48) ((with one 3)) + (9 + 18 + 36 + 72 + 144) ((with two 3’s)) = (1 + 2 + 4 + 8 + 16) (1 + 3 + 9).

σ(30) = (1 + 2)((from 2’s)) + (3 + 6) ((with one 3)) + (5 + 10 + 15 + 30) (with one 5) = (1 + 2 + 3 + 6) (1 + 5) = (1 + 2)(1 + 3)(1 + 5). End ex.

Recall (x^r + x^{r-1} + · · · + x + 1)(x-1) = x^{r+1} - 1. So 1 + x + · · · + x^r = \frac{x^{r+1}-1}{x-1}. So if n = ∏_{i=1}^r p_i^{a_i} (canon rep’n) then σ(n) = ∏_{i=1}^r \frac{p_i^{a_i+1}-1}{p_i-1}.

Ex 35. Find n such that σ(n) = 2n (perfect) σ(n) < 2n (deficient) σ(n) > 2n (abundant) (Concept of ab/de first described by Nicomachus around 100AD)

If a, b, c ∈ Z≥1 and a^2 + b^2 = c^2 then a, b, c is a Pythagorean triple. Famous: (3, 4, 5), 3^2 + 4^2 = 5^2. Note \((\frac{a}{c})^2 + (\frac{b}{c})^2 = 1\) so Pyth triple give us point \((\frac{a}{c}, \frac{b}{c})\) with rat’l coord’s on x^2 + y^2 = 1. Every Pyth triple gives a “rat’l point” on x^2 + y^2 = 1.

Conversely, a rational point on x^2 + y^2 = 1 give Pyth triples. E.g. (\frac{7\ell}{2\sqrt{13}})^2 + (\frac{28\ell}{2\sqrt{13}})^2 = 1 gives 75^2 + 2812^2 = 2813^2 and (75\ell)^2 + (2812\ell)^2 = (2813\ell)^2 for any \ell ∈ Z≥1. So if we can find all rational points on x^2 + y^2 = 1 can find all Pythagorean triples.

How find the rat’l pts: Fix base point (−1, 0) on x^2 + y^2 = 1. There is bijection between rational points on x^2 + y^2 = 1 other than (−1, 0) and rational numbers m by \((\frac{a}{c}, \frac{b}{c}) \mapsto \text{slope of line connecting } (−1, 0) \text{ and } (\frac{a}{c}, \frac{b}{c}). \) One direction easy. If \((\frac{a}{c}, \frac{b}{c})\) is a rational point then the slope connecting is rational. Other direction. Given m, a rational number, show the other point of intersection of y = m(x + 1) and x^2 + y^2 = 1 is a rational point.

Challenge me with an m with 0 < m < 1, not too awful.

To here, seventh lecture.

Do in general, restrict to 0 < m < 1. ((Talk through)).
DON’T LEAVE NOTES!!!!

Do generically: Let $0 < m < 1 \ (\cap \ \text{in Quad I}).$ Then $y = m(x+1)$ meets $x^2 + y^2 = 1$ where $x^2 + m^2(x+1)^2 = 1$ or $x^2 - 1 + m^2(x+1)^2 = 0$ or $(x+1)[(x-1) + m^2(x+1)] = (x+1)[(m^2+1)x + m^2 - 1] = 0.$ They meet where $x = -1$ (knew that) and where $x = \frac{-m^2}{m^2+1}$. What’s $y$-coor?

$$y = m(x+1) = m \left( \frac{1 - m^2}{m^2 + 1} + 1 \right) = m \left( \frac{1 - m^2 + m^2 + 1}{m^2 + 1} \right) = \frac{2m}{m^2 + 1}.$$  

Let $m = \frac{d}{e}$ with $d, e \in \mathbb{Z}_{\geq 1}$ and $d < e$ (since $0 < m < 1$) and $\gcd(d, e) = 1.$

$$x = \frac{1 - \frac{d^2}{e^2} + 1}{\frac{d^2}{e^2} + 1} = \frac{e^2 - d^2}{e^2 + d^2} = \frac{l(e^2 - d^2)}{l(e^2 + d^2)}$$  

for any $l \in \mathbb{Z}_{\geq 1}.$

Since $x^2 + y^2 = 1$ we have

$$\left( \frac{l(e^2 - d^2)}{l(e^2 + d^2)} \right)^2 + \left( \frac{l2ed}{l(e^2 + d^2)} \right)^2 = 1 \text{ or } [l(e^2 - d^2)]^2 + [l2ed]^2 = [l(e^2 + d^2)]^2.$$

Indeed, rational slope $m$ gave rational point.  
In addition, we get all Pyth triples this way: $((\text{BOX})) \ a = l(e^2 - d^2), \ b = l(2ed), \ c = l(d^2 + e^2)$ where $l, d, e \in \mathbb{Z}_{\geq 1}, \ 0 < d < e$ and $\gcd(d, e) = 1.$

<table>
<thead>
<tr>
<th>$\ell$</th>
<th>$d$</th>
<th>$e$</th>
<th>$l(e^2 - d^2)$</th>
<th>$l2ed$</th>
<th>$l(e^2 + d^2)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>3</td>
<td>8</td>
<td>6</td>
<td>10</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>5</td>
<td>12</td>
<td>13</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>4</td>
<td>15</td>
<td>8</td>
<td>17</td>
</tr>
<tr>
<td>1</td>
<td>3</td>
<td>4</td>
<td>7</td>
<td>24</td>
<td>25</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>5</td>
<td>24</td>
<td>10</td>
<td>26</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>5</td>
<td>21</td>
<td>20</td>
<td>29</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>2</td>
<td>6</td>
<td>8</td>
<td>10</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>2</td>
<td>9</td>
<td>12</td>
<td>15</td>
</tr>
</tbody>
</table>

Call Pyth triple $a, b, c$ primitive if $\gcd(a, b, c) = 1.$ If primitive, book uses $s, t$ not $d, e.$

Prop 36. Let $a, b, c$ be a Pythagorean triple. This triple is primitive if $\ell = 1, \ (d, e) = 1$ and one of $d, e$ is even and other is odd.

Pf. $\Rightarrow$. Assume $a, b, c$ is prim. So $(a, b, c) = 1.$ $l|a, l|b, l|c \Rightarrow l|(a,b,c) = 1 \Rightarrow l|1.$

Let $(d, e) = g.$ Since $g|d$ and $g|e$ we have $g|(a, b), g|e$ so $g|(a, b, c) = 1$ and $g = 1.$

If $d, e$ both odd or both even then $2|2de[a, 2|e^2 - d^2|b, 2|e^2 + d^2|a$ so $2|(a,b,c)$ so not primitive.  
$\Leftarrow$. Let $g = (a, b, c) \ ((\text{show } g = 1)).$ Assume $p$ is a prime with $p|g$. Then $p|g|a = e^2 - d^2$ and $p|g|c = e^2 + d^2$ so $p|a + c = 2d^2$ and $p|c - a = 2e^2.$ Case 1. $p = 2.$ This contradicts one of $\{e, d\}$ even, one is odd since $e^2 - d^2$ is odd. Case 2. $p \neq 2.$ Then (Thm 18) $p|d^2$ and $p|e^2$ so $p|d$ and $p|e$ and $p|(d, e) = 1,$ a contradiction.

9
In book, with prim triple \( x, y, z \) with \( x^2 + y^2 = z^2 \), \( x, z \) are odd, \( y \) is even.

Aside: Place Pythagorean triples “come from”. Let \( i = \sqrt{-1} \). \( \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \). \( N : \mathbb{Z}[i] \to \mathbb{Z} \) by \( N(a+bi) = (a+bi)(a-bi) = a^2+b^2 \). This norm multiplicative too. \( N(2+i) = 5 \) \((\text{write } e = 2, d = 1 \text{ above})\). \( 5^2 = N(2+i)N(2+i) = N((2+i)(2+i)) = N(3+4i) = 3^2 + 4^2 \). Similarly \( N(4+i) = 17 \) \((\text{write } e = 4, d = 1 \text{ above})\). \( 17^2 = N(4+i)N(4+i) = N((4+i)^2) = N(15+8i) = 8^2 + 15^2 \). Can combine: \( (3^2 + 4^2 = 5^2) \ast (5^2 + 12^2 = 13^2) = \ast \). \( N(3+4i) = 5^2, N(5+12i) = 13^2 \). So \( 65^2 = N((3+4i)(5+12i)) = N(-33+56i) = 33^2 + 56^2 \). (Group: Pyth triples \( a^2 + b^2 = c^2 \) where \( a, b > 0 \) \( \text{so } 3^2 + 4^2 = 5^2 \) and \( 4^2 + 3^2 = 5^2 \) different) \( \cong \) points in \( \mathbb{Q}(i) \) with abs value \( \frac{1}{i} \).

End aside. 3800 year old Babyl’n clay tablet had \( 15 \) Pyth triples including \( 12709^2 + 13500^2 = 18541^2 \).

Primes. Finding them. If \( m \) composite then \( \exists \) prime \( p|m \) with \( p \leq \ast \). Assume contrary \( m \) composite then \( m = p_1p_2 \cdots p_r, p_i \) primes, \( r \geq 2, p_i > \sqrt{m} \) so \( p_1p_2 > m \). So every composite \( \leq 100 \) divisible by prime \( \leq \sqrt{100} = 10 \).

Sieve of Eratosthenes 276 - 194 BC.

Thm 37. There are infinitely many primes (Euclid ? - 265 BC).

Euclid’s pf: (Contr’n) Assume there are finitely many primes and list all of them: \( p_1, \ldots, p_r \). Let \( A = p_1p_2 \cdots p_r + 1 \). From FTA \( \exists \) prime \( p|A \). Clearly \( p_i|p_1p_2 \cdots p_r \) so \( p_i|1 \), a contr’n. End pf.

Can we generate primes this way? Does \( p|\text{imply } 2 \cdot 3 \cdot 5 \cdots p_i+1 \) is prime for all \( i \)? No \( 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 59 \cdot 509 \).

Pf 2. ((Draw picture of \( y = \frac{1}{2} \) and rectangle base \([1, 2] \) height 1, base \([2, 3] \) height \( \frac{1}{2} \), etc.))

Recall \( \sum_{n=1}^{\infty} \frac{1}{2} > \int_{1}^{\infty} \frac{1}{x} \, dx = \lim_{b \to \infty} \ln(b) = \infty. \)

Let \( S_2 = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{6} + \frac{1}{9} + \frac{1}{12} + \cdots = \sum_{n=2 \cdot 3^j} \frac{1}{n}. \ S_3 \equiv \frac{1}{n} = \left( \frac{1}{1 \frac{1}{2}} \right) \left( \frac{1}{1 \frac{1}{3}} \right) \left( \frac{1}{1 \frac{1}{5}} \right). \)

So \( \infty = \sum_{n=1}^{\infty} \frac{1}{n} = \Pi_S \left( \left( \frac{1}{1 \frac{1}{2}} \right) \left( \frac{1}{1 \frac{1}{3}} \right) \left( \frac{1}{1 \frac{1}{5}} \right) \right) \).
Since $\prod_{\text{primes } p} \frac{1}{1-p} = \infty$ there must be infinitely many primes.

Lemma 38. If $a, b \in \mathbb{Z}$ then $(3a + 1)(3b + 1)$ is of the form $3n + 1$ for some $n \in \mathbb{Z}$.

Proof: $(3a + 1)(3b + 1) = 9ab + 3a + 3b + 1 = 3(3ab + a + b) + 1$.

Thm 39. There are infinitely many primes of the form $3^n + 2$.

Proof: (Contr’nation) Assume there are finitely many primes of form $3^n + 2$ and list all of them: $2, q_1, q_2, \ldots, q_r$. Let $A = 3q_1 q_2 \cdots q_r + 2$. By FTA $\exists$ prime $|A$. Note $A$ is odd so 2 $/\mid A$. Note $A$ is of the form $3m + 2$, so $3 \not/\mid A$. Lemma 38 tells us $A$ is not a product of primes of the form $3^a + 1$. So $A$ has a prime divisor $q_i$ of form $3^n + 2$. Since $q_i|A$ and $q_i|q_1 q_2 \cdots q_r$ we have $q_i|2$, a cont’n. End pf.

Dirichlet’s Theorem (1837) If $(a, d) = 1$ with $a, d \in \mathbb{Z}_{\geq 1}$ then there are infinitely many primes of the form $dn + a$ with $n \in \mathbb{Z}_{\geq 1}$.

Won’t prove.

Ex 40. We’ve proved there are $\infty$ many primes of form $3n + 2$. Proof of that type won’t show $\exists \infty$ many primes of form $3n + 1$. But since $(3, 1) = 1$, Dir’s thm says $\exists \infty$ many primes of form $3n + 1$.

A conseq of Dir’s Thm is that there are infinitely many primes of the form $12n + 7$.

Need $(a, d) = 1$. The sequence $8n + 6$ for $n > 0$ has no primes. End ex.

We have seen that the linear function $f(n) = 15n + 14$ for $n \in \mathbb{Z}_{\geq 1}$ has $\infty$ many prime outputs. How about quadratic fns?

Ex 41. Consider the poly $f(n) = n^2 - n + 41$ for $n \in \mathbb{Z}_{\geq 1}$. Note $f(1) = 41$, $f(2) = 43$, $f(3) = 47$, $f(4) = 53$, $f(5) = 61$, $f(6) = 71$, $f(7) = 83$, $f(8) = 97$, \ldots can this go on forever?

Conjecture: There are quadratic polynomials that take on $\infty$ many prime outputs (when the input is a positive integer).

Subconjecture: There are $\infty$ many primes of the form $n^2 + 1$. (5, 17, 37, 101, 197, 257, 401, \ldots ?)

Theorem 42. Every polynomial with integer coefficients takes on $\infty$ many composite values (for integer inputs).

Easy uninteresting pf.

Ex 43. \[
x \begin{array}{c|cccccccccccccc}
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\
x^2 + 1 & 1 & 2 & 5 & 10 & 17 & 26 & 37 & 50 & 65 & 82 & 101 & 122 & 145 & 170 \\
\end{array}
\]

Let $f = x^2 + 1$, then $f(2), f(7), f(12), \ldots, f(2 + 5k)$ all divisible by 5. Since $f(2) = 2^2 + 1 = 5$, we have $f(2 + 5k) = (2 + 5k)^2 + 1 = 2^2 + 4 \cdot 5k + (5k)^2 + 1 = (2^2 + 1) + 5n = 5 + 5n$ is divisible by 5. Pf of Thm 42 is formalization of this. End ex.

Let $\pi(x)$ denote the number of primes $\leq x$.

((At second column ask: What fraction, so 1/2.5))
<table>
<thead>
<tr>
<th>$x$</th>
<th>$\pi(x)$</th>
<th>$\frac{x}{\pi(x)}$</th>
<th>$\ln(x)$</th>
<th>error</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>4</td>
<td>2.5</td>
<td>2.30</td>
<td>8%</td>
</tr>
<tr>
<td>100</td>
<td>25</td>
<td>4.0</td>
<td>4.61</td>
<td>15%</td>
</tr>
<tr>
<td>1000</td>
<td>168</td>
<td>5.95</td>
<td>6.91</td>
<td>16%</td>
</tr>
<tr>
<td>10000</td>
<td>1229</td>
<td>8.14</td>
<td>9.21</td>
<td>13%</td>
</tr>
<tr>
<td>100000</td>
<td>9592</td>
<td>10.43</td>
<td>11.51 10%</td>
<td>8%</td>
</tr>
<tr>
<td>$10^6$</td>
<td>78498</td>
<td>12.74</td>
<td>13.82</td>
<td>8%</td>
</tr>
<tr>
<td>$10^9$</td>
<td>50847478</td>
<td>19.67</td>
<td>20.72</td>
<td>5%</td>
</tr>
</tbody>
</table>

Gets better for larger $x$.

Prime number theorem (1896).

$$
\lim_{x \to \infty} \frac{\pi(x)}{x/\ln(x)} = 1.
$$

So odds that a randomly chosen integer between 1 and $10^{10}$ is prime is about $1/\ln(10^{10}) \approx 1/23$.

If $p$ and $p + 2$ are prime, they are called twin primes. 3, 5, 17, 19, 101, 103, 123491, 123493.

Conjecture: There are infinitely many pairs of twin primes.

To here, tenth lecture

Thm 45. $\sum_{p \text{prime}} \frac{1}{p}$ diverges.

Brun’s Thm $\sum_{q \text{ twin prime}} \frac{1}{q}$ is finite.

Mersenne found that $2^n - 1$ prime for $n = 2, 3, 5, 7, 13, 17, 19$. Primes of the form $2^n - 1$ are called Mersenne primes. 47 are known. (Note $2^{11} - 1 = 23 \cdot 89$.)

Prop 46. Let $n \in \mathbb{Z}_{\geq 2}$. If $2^n - 1$ is prime, then $n$ is prime.

Pf. Let $n = mq$ with $m, q \in \mathbb{Z}_{>1}$. Then $2^n - 1 = (2^m - 1)(2^{m(q-1)} + 2^{m(q-2)} + \ldots + 1)$. Both $\geq 2$. End pf.

Prop 47. If $m^n - 1$ is prime with $m, n \in \mathbb{Z}_{>1}$ then $m = 2$.

Pf. Let $m > 2$. Then $m^n - 1 = (m - 1)(m^{n-1} + m^{n-2} + \ldots + 1)$ isn’t prime. End pf.

So only primes of the form $m^n - 1$ with $m, n \in \mathbb{Z}_{>1}$ are of the form $2^p - 1$ for $p$ prime and are called Mersenne primes. 46 are known.

The 46th is the largest known prime: $2^{43,112,607} - 1$. Has about 13 million digits.

For random integers, can test if prime or not if has up to 10000 digits. Since above of special form, there’s special primality test.

$n$ perfect if $\sigma(n) = 2n$ (sum of positive divisors). Examples: 6, 28, 496. (Euclid, 300 BC)

Theorem 48: If $2^p - 1$ is prime, then $2^{p-1}(2^p - 1)$ is perfect (Euclid) and all even perfect numbers are of this form (Euler, about 1760).

Proof. Assume $2^p - 1$ is prime. Recall

$$
\sigma \left( \prod p_i^{n_i} \right) = \prod \left( \frac{p_i^{n_i+1} - 1}{p_i - 1} \right)
$$
so

$$\sigma(2^{p-1}(2^p-1)^{\frac{1}{2}}) = \left(\frac{2^p-1}{2-1}\right) \left(\frac{(2^p-1)^2-1}{2^p-1-1}\right)$$

$$= (2^p-1)((2^p-1)+1) = (2^p-1)(2^p) = 2(2^{p-1}(2^p-1))$$

PREPARE: Assume \( n \) even and \( \sigma(n) = 2n \). Let \( n = 2^r \cdot m \) with \( m \) odd, \( r > 0 \). Now \( \sigma(n) = \sigma(2^r)\sigma(m) = \frac{2^{r+1}-1}{2-1}\sigma(m) = (2^{r+1}-1)\sigma(m) \). And \( \sigma(n) = 2n = 2^{r+1}m \).

So \( (2^{r+1}-1)\sigma(m) = 2^{r+1}m \). Since \( (2^{r+1}-1, 2^{r+1}) = 1 \) and \( 2^{r+1}-1|2^{r+1}m \) we have \( (2^{r+1}-1)|m \). So \( \frac{m}{2^{r+1}-1} \) is an integer, and a divisor of \( m \). Now \( \sigma(m) = \frac{2^{r+1}m}{2^{r+1}-1} = \frac{m(2^{r+1}-1)+m}{2^{r+1}-1} = m + \frac{m}{2^{r+1}-1} \).

Now \( \sigma(m) \) is the sum of ALL of \( m \)'s divisors. From above, \( \sigma(m) = m \) + “one other divisor of \( m \)”. So that divisor must be 1 and \( m \) must be prime. So \( m \) is prime and \( \frac{m}{2^{r+1}-1} = 1 \), we see \( m \) is of the form \( 2^{r+1} - 1 \). So \( n \) is of the form \( 2^r(2^{r+1} - 1) \) where \( 2^{r+1} - 1 \) is prime. From Prop 46, \( r + 1 \) is prime. End pf.

Conjecture: There are infinitely many even perfect numbers.

This is equivalent to the Conjecture: There are infinitely many Mersenne primes.

6 perfect, \( 6 = 2^1(2^2 - 1) \). 28 perfect, \( 28 = 2^2(2^3 - 1) \). 496 perfect, \( 496 = 2^4(2^5 - 1) \), 8128 perfect, \( 8128 = 2^6(2^7 - 1) \).

Conjecture: There are no odd perfect numbers.

Fermat noticed \( F(n) = 2^{2^n} + 1 \) prime for \( n = 0, 1, 2, 3 \) and \( 4 \). \( F(0) = 3, F(1) = 5, F(2) = 17, F(3) = 257, F(4) = 65537 \) and conjectured \( F(n) \) prime \( \forall n \in \mathbb{Z}_{\geq 0} \).

Current conjecture: \( F(n) \) composite for \( n > 4 \). Note \( F(5) = 641 \cdot 6700417 \) (Euler).

To here, eleventh lecture

Mod: (Invented by Gauss \( \approx 1750 \)). Start with calculator trick.

Modular arithmetic is a way of replacing \( \infty \) problems with finite problems.

If \( m \in \mathbb{Z}_{\geq 1} \) and \( m|a - b \) then say \( a \) is congruent to \( b \) modulo \( m \) and write \( a \equiv b \pmod{m} \).

Ex 49. \( 7 \equiv 3 \pmod{4}, 11 \equiv -1 \pmod{4} \).

\( a \equiv b \pmod{4} \) means \( a \) and \( b \) differ by a multiple of \( 4 \).

\( 11 = 2 \cdot 4 + 3 \). If \( a = qm + r \) with \( 0 \leq r < m \) then \( a \equiv r \pmod{m} \). Call \( r \) the least residue of \( a \pmod{m} \).

Working mod 4 breaks all integers into 4 (equivalence) classes: Each class contains exactly one from the set \( \{0, 1, 2, 3\} \) (poss remainders). End ex.

Prop 49.5. \( a \equiv b \pmod{m} \) iff \( a \) and \( b \) have same remainder when divided by \( m \).

Pf: Easy.

So every integer is congruent modulo \( m \) to exactly one integer in set \( \{0, 1, 2, \ldots, m - 1\} \). That set is called the least residue system modulo \( m \).

If \( a > m \) then to reduce \( a \pmod{m} \) is to find \( r \) with \( r \) in the least residue system mod \( m \) with \( a \equiv r \pmod{m} \).

On calculator, to reduce 353\( \pmod{47} \). Do 353 \(-\) 47 = 7.5106 \ldots, –7 = .5106 \ldots, \( \times 47 = 24 \). Why work?
As set of integers \( \{a_0, a_1, \ldots, a_{m-1}\} \) which is \( \equiv \{0, 1, \ldots, m-1\} \mod m \) is called a complete residue system. So \( \{-2, 8, 11, 101\} \) is a crs mod 4.

Which integers are \( 1 \mod 2 \)? \( 0 \mod 2 \)?

Describe positive integers \( \equiv 7 \mod 10 \).

Negative?

Prop 50. \( \equiv \mod m \) is an equivalence relation. I.e. if \( a, b, c \in \mathbb{Z} \) then

i) \( a \equiv a \mod m \).

ii) \( a \equiv b \mod m \Rightarrow b \equiv a \mod m \).

iii) \( a \equiv b \mod m \) and \( b \equiv c \mod m \Rightarrow a \equiv c \mod m \).

Pf. i) \( a - a = 0 \cdot m \).

ii) \( m|(a - b) \Rightarrow m|\ -1(a - b) = b - a \).

iii) \( m|a - b, m|c - b \Rightarrow m|(a - b) + (b - c) = a - c \).

((Clocks work mod 12. 3 hours after 10 is 1 since 3 + 10 \( \equiv 1 \mod 12 \)).)

+, −, · work well mod \( m \) for a fixed \( m \):

(( do diagram. 18, 32 \( \mod \nabla 11 \) and + .))

Prop 51. If \( a \equiv b \mod m \) and \( c \equiv d \mod m \) then

i) \( a + c \equiv b + d \mod m \)

ii) \( a - c \equiv b - d \mod m \)

iii) \( ac \equiv bd \mod m \)

Pf i) \( m|(a - b) \Rightarrow m|(a + c) - (b + d) \).

ii) \( m|(a - b) - (c - d) = (a - c) - (b - d) \).

iii) \( \exists k, l \) such that \( a - b = km, c - d = lm, a = km + b, c = lm + d \). \( ac - bd \equiv m(ac - bd) \).

Cor 52. If \( a \equiv b \mod m \) and \( n \in \mathbb{Z}_{\geq 0} \) then \( a^n \equiv b^n \mod m \).

Follows from Prop 51 iii).

Ex 53: Old prob: Show all squares of form \( 4n \) or \( 4n + 1 \). i.e. all squares \( \equiv 0 \) or \( 1 \mod 4 \).

Let \( x \in \mathbb{Z} \). Then \( x \equiv 0, 1, 2 \) or \( 3 \mod 4 \). So \( x^2 \equiv 0^2, 1^2, 2^2 \) or \( 3^2 \equiv 0, 1, 0 \mod 4 \).

Ex 54. Old prob: Show \( 5|2^{4n+2} + 1 \) for each \( n \in \mathbb{Z}_{\geq 1} \). Note \( 5|t \equiv 0 \mod 5 \). \( 2^{4n+2} + 1 = 2^{4n} + 1 = (2^2)^n + 1 \equiv 1^n \cdot 4 + 1 \equiv 0 \mod 5 \).

To here, twelfth lecture

Ex. 55. Find least residue of \( (399)^{83} - (62)^{83} + (78)(59) \mod 8 \). Don’t reduce exponents.

((To here can assign 4.1 homework))

Math 52. \( \mathbb{Z} \) is a group under +. \( 4\mathbb{Z} \) is a subgroup. 4 cosets: \( 0 + 4\mathbb{Z} = 4\mathbb{Z} \) \( \{n \in \mathbb{Z} | n \equiv 0 \mod 4\} \) = \( \{4k | k \in \mathbb{Z}\} \).

\( 1 + 4\mathbb{Z} \) \( \equiv \{n \in \mathbb{Z} | n \equiv 1 \mod 4\} \equiv \{4k + 1 | k \in \mathbb{Z}\} \),

\( 2 + 4\mathbb{Z}, 3 + 4\mathbb{Z} \).

Cosets form a group denoted \( \mathbb{Z}/4\mathbb{Z} \) of 4 elements under addition \((2 + 4\mathbb{Z}) + (3 + 4\mathbb{Z}) = \ldots \).

We have \( \mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}_4 = \{0, 1, 2, 3\} \) by \( r + 4\mathbb{Z} \rightarrow r \). Recall in \( \mathbb{Z}_4 \) do addition mod 4.

For \( n \in \mathbb{Z}, n \geq 2 \) can also multiply in \( \mathbb{Z}_n \). Division is strange, we’ll do later.
Make a mult’n table for multiplication mod 6 (in $\mathbb{Z}_6$).

Ex 56. $8 \cdot 2 \equiv 3 \cdot 2 (\text{mod } 10)$. Cancel 2’s? No. What can you do? $16 \equiv 6 (\text{mod } 10)$. $8 \cdot 2 \equiv 3 \cdot 2 (\text{mod } 5 \cdot 2)$ and $8 \equiv 3 (\text{mod } 5)$.

Prop 57. If $c \in \mathbb{Z}_{>0}$ and $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}_{\geq 2}$ then $ac \equiv bc (\text{mod } mc) \Rightarrow a \equiv b (\text{mod } m)$.

Pf. $c \neq 0, mc|ac - bc \Rightarrow m|a - b$. (Prop 4 iv) End pf.

Ex 58. $6 \cdot 20 = 120$. Which positive integers, when mult’d by 6, have the same last 2 digits? $x, y \in \mathbb{Z}_{\geq 1}$ have same last two digits iff $x \equiv y (\text{mod } 100)$. Want $6x \equiv x (\text{mod } 100)$ or $5x \equiv 0 (\text{mod } 100)$ or $5x \equiv 5 \cdot 0 (\text{mod } 5 \cdot 20)$ or $x \equiv 0 (\text{mod } 20)$ or $20|x$. I.e. $6 \cdot 40 = 240, 6 \cdot 60 = 360$, etc.

Ex 59. $53 \equiv 5 (\text{mod } 3), 53 \equiv 5 (\text{mod } 4)$. So $53 \equiv 5$??

Thm 60. If $a \equiv b (\text{mod } m)$ and $a \equiv b (\text{mod } n)$ and $(m, n) = 1$ then $a \equiv b (\text{mod } mn)$.

Pf. We have $m|a - b, n|a - b$ and $(m, n) = 1$ so $mn|a - b$. (Thm 20).

Ex 61. $5^2 - 1 = 24, 7^2 - 1 = 48, 11^2 - 1 = 120$. Pattern?

Cor 62. If $p > 3$ is prime then $p^2 \equiv 1 (\text{mod } 24)$.

Pf. If $p > 3$ then $p \equiv 1, 2 (\text{mod } 3)$ so $p^2 \equiv 1^2, 2^2 \equiv 1, 1 (\text{mod } 3)$. If $p > 3$ then $p \equiv 1, 3, 5, 7 (\text{mod } 8)$ so $p^2 \equiv 1^2, 3^2, 5^2, 7^2 \equiv 1, 1, 1, 1 (\text{mod } 8)$. So $p^2 \equiv 1 (\text{mod } 3)$ and $p^2 \equiv 1 (\text{mod } 8)$ and $(3, 8) = 1$ so from Thm 60, $p^2 \equiv 1 (\text{mod } 24)$. End pf.

To here, thirteenth lecture.

Now done with material appearing on midterm next Friday.

Prop 63. Let $n = a_m 10^m + a_{m-1} 10^{m-1} + \ldots + a_1 10 + a_0$ with $0 \leq a_i \leq 9$.

i) $n \equiv \sum a_i (\text{mod } 9)$ so $9|n$ if $9|\sum a_i$.

ii) $n \equiv \sum a_i (\text{mod } 3)$ so $3|n$ iff $3|\sum a_i$.

ii) $n \equiv \sum (-1)^i a_i (\text{mod } 11)$ so $11|n$ iff $11|\sum (-1)^i a_i$.

Ex 64. Does $3|1705296$? Does $9|1705296$? Add what so divisible by 9?

Does $11|6565405$? Is $606144$ divisible by 7?

Thm 65. Let $m \in \mathbb{Z}_{>1}, a \in \mathbb{Z}$. The equation $ax \equiv 1 (\text{mod } m)$ is solvable iff $(a, m) = 1$.

Pf. $\Rightarrow$: Let $ax \equiv 1 (\text{mod } m)$ and $g = (a, m)$. Thus $g|m$ and $m|ax - 1$ so $g|ax - 1$. Also $g|a$ so $g|ax$ and thus g|1 so g = 1. $\Leftarrow$: If $(a, m) = 1$ then $\exists x, y \in \mathbb{Z}$ such that $ax + my = 1$ so $ax + my \equiv 1 (\text{mod } m)$ so $ax + 0(y) \equiv 1 (\text{mod } m)$. End pf.

If $(a, m) = 1$ then say a is invertible mod m (or in $\mathbb{Z}/m\mathbb{Z}$ or if $0 \leq a < m$ then in $\mathbb{Z}_m$). If $ab \equiv 1 (\text{mod } m)$ then say $b \equiv a^{-1}$ or $\frac{1}{a}(\text{mod } m)$ (or in $\mathbb{Z}/m\mathbb{Z}$, etc.).

Ex 66. $2 \cdot 3 \equiv 1 (\text{mod } 5)$. So say $2 \equiv \frac{1}{3} \equiv 3^{-1} (\text{mod } 5)$ and $3 \equiv \frac{1}{2} \equiv 2^{-1} (\text{mod } 5)$.

Cor 67. If $(a, m) = 1$ and $b \equiv c (\text{mod } m)$ then $\frac{b}{a} \equiv \frac{c}{a} (\text{mod } m)$. (I.e. $b \cdot \frac{1}{a} \equiv c \cdot \frac{1}{a} (\text{mod } m)$). (Leave, don’t $a \equiv d (\text{mod } m)$)

Ex 68. Simplify $\frac{2}{3} (\text{mod } 10)$.

Ex 69. Solve $9x \equiv 1 (\text{mod } 29)$. (Find $9^{-1}$ in $\mathbb{Z}_{29}$).
29 = 3 \cdot 9 + 2, 9 = 4 \cdot 2 + 1. 1 = 9 - 4 \cdot 2 = 9 - 4(29 - 3 \cdot 9) = 13 \cdot 9 - 4 \cdot 29 = 1. So \ 1 \equiv 13 \cdot 9 - 4 \cdot 29 \pmod {29}.
1 \equiv 13 \cdot 9 \pmod {29}. So \ x = 13 \pmod {29}). \ 9^{-1} = \frac {1} {9} \equiv 13 \pmod {29}.

To here, fourteenth lecture

Ex 70. Find 39^{-1} \pmod {29}.

Ex 71. In \ \mathbb {Z} _{15} = \{0, 1, \ldots, 14\} which invertible? The ones rel prime to 15: 1, 2, 4, 7, 8, 11, 13, 14. Inverses:
1 \cdot 1 = 1, \quad 1 = (-1)(-1) = 14 \cdot 14.
2 \cdot 8 = 1, \quad 1 = (-2)(-8) = 13 \cdot 7.
4 \cdot 4 = 1, \quad 1 = (-4)(-4) = 11 \cdot 11.

Denote set \{1, 2, 4, 7, 8, 11, 13, 14\} by \mathbb {Z} _{15}^\ast. \text{ End ex.}

\mathbb {Z} _{m}^\ast = \{x \in \mathbb {Z} _{m} | (x, m) = 1\}.

\mathbb {Z} _{m}^\ast \text{ is a group under multiplication ((Don’t prove)). Iden is 1. Here we } \times, \div \text{ don’t +, -.}

Size of \mathbb {Z} _{m}^\ast = \# \{x \in \mathbb {Z} _{m} | (x, m) = 1\} \text{ is denote } \phi (m). \text{ This is the Euler phi function (or totient fcn).}

Ex 72. \phi (15) = 8, \phi (2), \phi (3), \phi (4), \ldots, \phi (13). \text{ End ex.}

Lemma 73. If \ p \text{ is prime then } \phi (p) = p - 1.

Ex 74. \mathbb {Z} _{3}^\ast = \{1, 2\}, \mathbb {Z} _{5}^\ast = \{1, 2, 4, 5, 7, 8\} = \mathbb {Z} _{9} \setminus 3\mathbb {Z} _{9}.
\mathbb {Z} _{27}^\ast = \{1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26\} = \mathbb {Z} _{27} \setminus 3\mathbb {Z} _{27}. \text{ End ex.}

Lemma 75. If \ p \text{ is prime then } \phi (p^{r}) = p^{r} - p^{r-1} = p^{r-1}(p - 1).

Lemma 76. (justify later). If \ n, m \in \mathbb {Z} _{\geq 1} \text{ and } (m, n) = 1 \text{ then } \phi (mn) = \phi (m)\phi (n).

Ex 77. Find \phi (90000). 90000 = 2^{4} \cdot 3^{2} \cdot 5^{4}. \text{ So } \phi (90000) = \phi (2^{4})\phi (3^{2})\phi (5^{4}) = 2^{4}(2 - 1)3^{1}(3 - 1)5^{4}(5 - 1) = 8 \cdot 1 \cdot 3 \cdot 2 \cdot 125 \cdot 4 = 24000.

Thm 78. If \ n \in \mathbb {Z} _{2} \text{ and } \prod p_{i}^{n_{i}} \text{ its canon rep’n then } \phi (n) = \prod p_{i}^{n_{i}-1}(p_{i} - 1).

Theorem (Euler). If \ (c, m) = 1 \text{ then } c^{\phi (m)} \equiv 1 \pmod {m}.

Pf. Since multiplication works well mod \ m \text{ wlog can assume } c \text{ already reduced so } c \in \mathbb {Z} _{m}^\ast. \text{ We know } \phi (m) = \# \mathbb {Z} _{m}^\ast. \text{ A corollary of Lagrange’s thm ((size of sbgp of finite gp)) says that in a finite gp, an element to the power of the order of the group is the identity. End pf.}

Corollary (Fermat’s little Thm version 1) If \ p \text{ prime, } c \in \mathbb {Z} \text{ and } p \nmid c \text{ then } c^{p-1} \equiv 1 \pmod {p}.

Ex. 79. So \ 4^{6} \equiv 1 \pmod {7}.

Corollary (Fermat’s little Thm version 2) If \ p \text{ prime and } c \in \mathbb {Z} \text{ then } c^{p} \equiv c \pmod {p}.

Corollary 80. If \ (c, m) = 1 \text{ (← important!)}, d, e \in \mathbb {Z} _{\geq 0}, \text{ and } d \equiv e(\text{mod } \phi (m)) \text{ then } c^{d} \equiv c^{e} \pmod {m}.

Pf. WLOG let \ d \geq e. \text{ Then } \exists k \in \mathbb {Z} \text{ s.t. } \ d - e = k\phi (m). \text{ So } d = e + k\phi (m). \text{ So } c^{d} \equiv c^{e+k\phi (m)} \equiv c^{e}c^{k\phi (m)} \equiv c^{e}(c^{\phi (m)})^{k} \equiv c^{e} \cdot 1 \equiv c^{e} \pmod {m}. \text{ End pf.}

Ex 81. Find the last digit of 7^{85322}. 

16
Mod 10:

\[
\begin{align*}
7^1 &\equiv 7 & 7^2 &\equiv 9 & 7^3 &\equiv 3 & 7^4 &\equiv 1 \\
7^5 &\equiv 7 & 7^6 &\equiv 9 & 7^7 &\equiv 3 & 7^8 &\equiv 1 \\
7^9 &\equiv 7 & 7^{10} &\equiv 9 & 7^{11} &\equiv 3 & 7^{12} &\equiv 1 \\
\vdots & & & & & & & \\
7^{85320} &\equiv 9
\end{align*}
\]

To here, fifteenth lecture

Better: \(\phi(10) = \phi(5)\phi(2) = (5-1)(2-1) = 4\). 85322 \equiv 2(\text{mod} 4) . Since \((7,10) = 1\), from Cor 80 \(7^{85322} \equiv 7^2 \equiv 49 \equiv 9(\text{mod} 10)\). So ends in a 9. End ex.

Ex. 82. What are last two digits of 99^3? Find 99^3(\text{mod} 100). Since 3 < \phi(100), Cor 80 useless. Trick: 99^3 \equiv (-1)^3 \equiv -1 \equiv 99(\text{mod} 100).

Linear modular equations.

Ex. 83. Solve 3x \equiv 2(\text{mod} 10).

Solve 4x \equiv 8(\text{mod} 10): Book: \(x \equiv 2,7(\text{mod} 10)\). Me: \(x \equiv 2(\text{mod} 5)\).

\(4x \equiv 7(\text{mod} 10)\).

23x \equiv 12(\text{mod} 10).

End ex.

Let \(a,b \in \mathbb{Z}, m \in \mathbb{Z}_{\geq 2}\) be fixed. Let \(g = (a,m)\). Consider eq’n \(ax \equiv b(\text{mod } m)\).

Prop 84. \(ax \equiv b(\text{mod } m)\) has a solution iff \(g|b\).

Pf. \(\Rightarrow\) Let \(g\) be a sol’n. We have \(agy \equiv b(\text{mod } m)\). So \(m|ay - b\). Since \(g|m\) we have \(g|ay - b\). Since \(g|a\) we have \(g|ay\) so \(g|b\).

\(\Leftarrow\) Assume \(g|b\). So \(b = kg\) for some \(k \in \mathbb{Z}\). Since \(g = (a,m)\), \(\exists v, x \in \mathbb{Z}\) s.t. \(g = av + mx\). So \(kg = avk + mxk\) or \(mxk = a(vk) - b\). So \(m|a(vk) - b\). So \(a(vk)\) \(\equiv b(\text{mod } m)\) and so \(ay \equiv b(\text{mod } m)\) has a sol’n. End pf.

If \(g|b\) then \(ax \equiv b(\text{mod } m) \Leftrightarrow m|ax - b \Leftrightarrow (\text{Prop } 4) \frac{m}{g} | \frac{a}{g}x - \frac{b}{g} \Leftrightarrow \frac{a}{g}x \equiv \frac{b}{g}(\text{mod } \frac{m}{g})\).

Note \((\frac{a}{g}, \frac{m}{g}) = 1\) so \(\frac{a}{g}\) is invertible mod \(\frac{m}{g}\). We have \(\frac{a}{g}x \equiv \frac{b}{g}(\text{mod } \frac{m}{g}) \Leftrightarrow x \equiv (\frac{a}{g})^{-1} \frac{b}{g}(\text{mod } \frac{m}{g})\).

Ex. 85. Solve 15x \equiv 10(\text{mod } 55). Well (15,55) = 5. So this same as 3x \equiv 2(\text{mod } 11) or \(x \equiv 3^{-1} \cdot 2(\text{mod } 11)\).

Clearly 3 \cdot 4 \equiv 1(\text{mod } 11) so 3^{-1} \equiv 4(\text{mod } 11)\). So \(x \equiv 4 \cdot 2 \equiv 8(\text{mod } 11)\). (Check 3 \cdot 8 \equiv 2(\text{mod } 11), yup!).

The solution can be written \(x \equiv 8(\text{mod } 11)\) OR \(\{11n + 8 | n \in \mathbb{Z}\}\) OR \(x \equiv 8,19,20,31,42(\text{mod } 55)\). Note # of sol’ns mod 55 is 5 = (15,55). End Ex.

Ex. 86. Buy a $9.40 BART ticket from machine. You have dimes and quarters. How many ways can you do it? Parametrize the solutions. \(10d + 25q = 940, d,q \in \mathbb{Z}_{\geq 0}\).

First divide through by 5: 2d + 5q = 188. Reduce mod smaller coefficient to get rid of unknown. 5q \equiv 188(\text{mod } 2)\) or \(q \equiv 0(\text{mod } 2)\).

So \(q = 2n\) for \(0 \leq n \leq 18\). So 19 solutions. Then plug in \(2d = 188 - 5q = 188 - 5(2n) = 188 - 10n\) so \(d = 94 - 5n\). So \((d,q) = (94 - 5n,2n)\) for \(0 \leq n \leq 18\).

To here, sixteenth lecture

Chinese Remainder Theorem.

Ex. 87. Have x people. Break into teams of 9, \(\exists 3\) left over. . . . teams of 10, \(\exists 3\) left over. . . . teams of 11, \(\exists 7\) left over. What’s smallest possible \(x\)?

\(x \equiv 4(\text{mod } 9)\)

\(x \equiv 3(\text{mod } 10)\)
\[ x \equiv 7 \pmod{11}. \]

Game plan: \[ x = 4 \cdot 10 \cdot 11 \cdot ??? + 3 \cdot 9 \cdot 11 \cdot ??? + 7 \cdot 9 \cdot 10 \cdot ???. \] First \[ ??? = (10 \cdot 11)^{-1} \pmod{9}. \]

\[ x = 4 \cdot 10 \cdot 11 \cdot 5 + 3 \cdot 9 \cdot 11 \cdot 9 + 7 \cdot 9 \cdot 10 \cdot 6 = 8653. \] \[ x \equiv 8653 \pmod{9 \cdot 10 \cdot 11} = 990 \]

\[ x \equiv 733 \pmod{9 \cdot 10 \cdot 11}. \]

Note (use tricks)
\[ 733 \equiv \begin{align*} & \equiv 4 \pmod{9} \\ & \equiv 3 \pmod{10} \\ & \equiv 7 \pmod{11} \end{align*} \]

Recall \[ m_1 \mid x \Rightarrow m \mid x \Rightarrow a \equiv b \pmod{mn} \Rightarrow a \equiv b \pmod{m}. \] Thus \[ a \equiv b \pmod{m}. \]

Existence of solution from alg’m:
\[ x \equiv a_1 \left( \prod_{i=1}^{r} \frac{m_i}{m_1} \right) b_1 + \ldots + a_r \left( \prod_{i=1}^{r} \frac{m_i}{m_r} \right) b_r \pmod{\prod_{i=1}^{r} m_i} \]

Uniqueness from the following theorem:

Product of groups (under +) \[ G \times H = \{ (g, h) \mid g \in G, h \in H \}. \]

Thm 88. (Gp theory version of CRT) If \( m, n \in \mathbb{Z}_{\geq 2} \) and \( (m_i, m_j) = 1 \) \( \forall i \neq j \). Then \[ x \equiv a_1 \pmod{m_1}, \ldots, x \equiv a_r \pmod{m_r} \] has a unique solution \( \pmod{m_1m_2 \cdots m_r} \). End Thm.

Will prove soon. ((First make it more concrete with examples.))

These are gps under +. \((0,0)\) is identity of \( \mathbb{Z}_m \times \mathbb{Z}_n \).

\[ \mathbb{Z}_{10} \cong \mathbb{Z}_2 \times \mathbb{Z}_5 \]

<table>
<thead>
<tr>
<th>( Z_{10} )</th>
<th>( \mathbb{Z}_2 \times \mathbb{Z}_5 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>(0,0)</td>
</tr>
<tr>
<td>1</td>
<td>(1,1)</td>
</tr>
<tr>
<td>2</td>
<td>(0,2)</td>
</tr>
<tr>
<td>3</td>
<td>(1,3)</td>
</tr>
</tbody>
</table>

Ex. 89. 4 \( \mapsto \) (0,4) 5 \( \mapsto \) (1,0) 6 \( \mapsto \) (0,1) 7 \( \mapsto \) (1,2) 8 \( \mapsto \) (0,3) 9 \( \mapsto \) (1,4)

Connect to CRT alg’m: Solve \( x \equiv 1 \pmod{2} \) and \( x \equiv 2 \pmod{5} \). \( f^{-1}(1, 2) = 7 \).

Verify it’s a hom in one case: In \( \mathbb{Z}_{10} \), \( 3 + 9 = 2 \). Note \( 3 \mapsto (1, 3) \), \( 9 \mapsto (1, 4) \) and \( 2 \mapsto (0, 2) \). In \( \mathbb{Z}_2 \times \mathbb{Z}_5 \) we have \((1, 3) + (1, 4) = (0, 2)\). Yup.
Ex. 90 Let’s rethink Ex 87.
\[\mathbb{Z}/90\mathbb{Z} \cong \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/110\mathbb{Z}\]
\[733 \mapsto (4, 73)\]
\[\cong \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}\]
\[\mapsto (4, 3, 7)\]

Pf of Thm 88.

i) Prove \(f\) is a homomorphism. This follows immediately from the facts that \(a \equiv b \pmod{mn}\) implies \(a \equiv b \pmod{m}\) and \(a \equiv b \pmod{n}\) and mod respects addition.

ii) Prove \(f\) is one-to-one. Recall that for a hom, suff to show that kernel is trivial, i.e. if \(f(x) = 0\) then \(x = 0\).
Let \(f(x) = (0, 0)\). Then \(m|x\) and \(n|x\). Since \((m, n) = 1\) we have \((\text{Thm} 20)\ mn|x\ or \(x \equiv 0 \pmod{mn}\).

iii) Prove \(f\) is onto. Follows from the existence of the CRT algm.

End pf.

Thm 91. Assume \(m, n \in \mathbb{Z}_{\geq 1}\) and \((m, n) = 1\). The map \(h : \mathbb{Z}_{mn}^* \cong \mathbb{Z}_m^* \times \mathbb{Z}_n^*\) by \(h(x) = (x \pmod{m}, x \pmod{n})\) is a well-defined isomorphism of groups. End Thm. Won’t prove. Proof similar.

Ex 91.5 \(\mathbb{Z}_5^* \cong \mathbb{Z}_3^* \times \mathbb{Z}_5^*\).

<table>
<thead>
<tr>
<th>(\mathbb{Z}_5^*)</th>
<th>(\mathbb{Z}_3^* \times \mathbb{Z}_5^*)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>(1, 1)</td>
</tr>
<tr>
<td>2</td>
<td>(2, 2)</td>
</tr>
<tr>
<td>4</td>
<td>(1, 4)</td>
</tr>
<tr>
<td>7</td>
<td>(1, 2)</td>
</tr>
<tr>
<td>8</td>
<td>(2, 3)</td>
</tr>
<tr>
<td>11</td>
<td>(2, 1)</td>
</tr>
<tr>
<td>13</td>
<td>(1, 3)</td>
</tr>
<tr>
<td>14</td>
<td>(2, 4)</td>
</tr>
</tbody>
</table>

Check hom in one case. \(2 \cdot 13 \equiv 11 \leftrightarrow (2, 2)(1, 3) = (2, 1)\).

Cor 92. If \(m, n \in \mathbb{Z}_{\geq 1}\) and \((m, n) = 1\) then \(\phi(mn) = \phi(m)\phi(n)\).

Pf. Since \(\mathbb{Z}_{mn}^* \cong \mathbb{Z}_m^* \times \mathbb{Z}_n^*\), we have \(\phi(mn) = |\mathbb{Z}_{mn}^*| = |\mathbb{Z}_m^* \times \mathbb{Z}_n^*| = |\mathbb{Z}_m^*||\mathbb{Z}_n^*| = \phi(m)\phi(n)\).

What is CRT good for: Need to solve a problem \(\pmod{mn}\) where \((m, n) = 1\). First solve \(\pmod{m}\), then \(\pmod{n}\) and glue solutions together with CRT alg’n.

Ex 92.5 Find all solutions to \(x^2 = 1 \pmod{77}\). Saw in HW that \(x^2 \equiv 1 \pmod{p}\) (odd prime), has exactly two solutions: \(x \equiv \pm 1 \pmod{p}\). But \(77 = 7 \cdot 11\). By CRT, \(x^2 \equiv 1 \pmod{77}\) iff \(x^2 \equiv 1 \pmod{7}\) and \(x^2 \equiv 1 \pmod{11}\).

Now \(x^2 \equiv 1 \pmod{7}\) has solutions \(x \equiv \pm 1 \pmod{7}\) and \(x^2 \equiv 1 \pmod{11}\) has solutions \(x \equiv \pm 1 \pmod{11}\). So \(x^2 \equiv 1 \pmod{77}\) has 2 · 2 solutions. First: \(x \equiv 1 \pmod{7}\) and \(x \equiv 1 \pmod{11}\) so \(x \equiv 1 \pmod{77}\). Second: \(x \equiv -1 \pmod{7}\) and \(x \equiv -1 \pmod{11}\) so \(x \equiv -1 \pmod{77}\). Third: \(x \equiv 1 \pmod{7}\) and \(x \equiv -1 \equiv 10 \pmod{11}\). To get this solution, we can use the CRT algorithm or, since 7 and 11 are small, note \(x \equiv 10 \pmod{11}\) means \(x = 11k + 10\). So \(x = 10 \equiv 3 \pmod{7}\), \(x = 21 \equiv 0 \pmod{7}\), \(x = 32 \equiv 4 \pmod{7}\), \(x = 43 \equiv 1 \pmod{7}\). So we have \(x \equiv 43 \pmod{77}\). Since \(43^2 \equiv 1 \pmod{77}\) then \(x \equiv -43 \equiv 34\) is a solution as well. So the four solutions are \(x \equiv 1, 34, 43, 76 \pmod{77}\).

Ex 93.

Consider equation \(x^2 + 2x + 3 = 0\)
Consider equation $x^3 + 2 = 0$

<table>
<thead>
<tr>
<th>Mod</th>
<th>2</th>
<th>3</th>
<th>5</th>
<th>7</th>
<th>11</th>
<th>13</th>
<th>17</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sol’n’s</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>7</td>
<td>0</td>
</tr>
<tr>
<td># Sol’n’s</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
</tbody>
</table>

Seems mod primes that # sol’n’s is $\leq$ degree.

Not true for composite: Recall earlier example: $x^2 - 1 \equiv 0 \mod 77$ has four solutions.

Ex 94. How many sol’n’s to $x^2 + 2x + 3 \equiv 0 \mod 33$? According to CRT, $x^2 + 2x + 3 \equiv 0 \mod 3$ iff $x^2 + 2x + 3 \equiv 0 \mod 11$. So $x \equiv 0, 1 \mod 3$ and $x \equiv 2, 7 \mod 11$ so $x \equiv 18, 24, 7 \mod 33$. End 94.

Wilson’s Thm: (Proved by Lagrange) If $p$ is prime then $(p-1)! \equiv -1 \mod p$.

Ex 95. $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8 \cdot 9 \cdot 10 \equiv -1 \mod 11$.

Why? $1 \cdot 10 \cdot 2 \cdot 6 \cdot 3 \cdot 4 \cdot 5 \cdot 9 \cdot 7 \cdot 8 \equiv 1 \cdot (-1) \cdot 1 \cdot 1 \cdot 1 \equiv -1 \mod 11$.

So other $p - 3$ elements can be paired off: $\alpha, \alpha^{-1}$. Can rearrange $1, 2, \ldots, p-1$ as $1, p-1, 2, p-2, \ldots$. So $(p-1)! \equiv 1(p-1)^{(p-3)/2} \equiv -1 \mod p$. End pf.

Example 96. Fibonacci numbers: $F_0 = 0, F_1 = 1$. For $n \in \mathbb{Z}_{\geq 2}$, $F_n = F_{n-1} + F_{n-2}$.

<table>
<thead>
<tr>
<th>$n$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
</tr>
</thead>
<tbody>
<tr>
<td>$F_n$</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>5</td>
<td>8</td>
<td>13</td>
<td>21</td>
<td>34</td>
<td>55</td>
<td>89</td>
<td>144</td>
<td>233</td>
<td>377</td>
</tr>
</tbody>
</table>

Prop 97.

$$F_n = \frac{1}{\sqrt{5}} \left[ \left( \frac{1 + \sqrt{5}}{2} \right)^n - \left( \frac{1 - \sqrt{5}}{2} \right)^n \right]$$

Pf. Easy induction.
Find a formula for $F_n$ mod 11. Find $\sqrt{5}$ (mod 11): Solve $x^2 \equiv 5$ (mod 11). $x = \pm 4 \equiv 4, 7$ (mod 11). Can say $\sqrt{5} \equiv 4$ (mod 11).

$$F_n = \frac{1}{4} \left[ \left( \frac{1+4}{2} \right)^n - \left( \frac{1-4}{2} \right)^n \right] \equiv 3[8^n - 4^n] \text{ (mod 11)}$$

So $F_0 \equiv 3[1 - 1] \equiv 0$ (mod 11), $F_1 \equiv 3[8 - 4] \equiv 1$ (mod 11). Let $p = 11$.

Note $F_{10} = F_{p-1} \equiv 3[8^{10} - 4^{10}] \equiv 3[8^{p-1} - 4^{p-1}] \text{ Fermat } \equiv 3[1 - 1] \equiv F_0 \equiv 0$ (mod 11).

Note $F_{11} = F_p \equiv 3[8^{11} - 4^{11}] \equiv 3[8^p - 4^p] \text{ Fermat } \equiv 3[8 - 4] \equiv F_1 \equiv 1$ (mod 11).

Since $F_{10} \equiv F_0$ and $F_{11} \equiv F_1$ and $F_{n} = F_{n-1} + F_{n-2}$ will cycle. ((Continue table above)). End ex.

Prop 99. If $p \neq 2, 5$ ((denom)) and $x^2 \equiv 5 \text{ (mod p)}$ has a sol’n, then $F_{p-1} \equiv 0 \text{ (mod p)}$ and $F_p \equiv 1 \text{ (mod p)}$.

Cor 100. If $p > 5$ and $x^2 \equiv 5 \text{ (mod p)}$ has a sol’n then $p|F_{p-1}$.

Cor 101. If $p > 5$ and $x^2 \equiv 5 \text{ (mod p)}$ has a sol’n then reduc’n of Fibo seq mod p will repeat every $p - 1$ terms.

Ex 102. $6^2 \equiv 5 \text{ (mod 31)}$. So $31|F_{30} = 382040 = 31 \cdot 26840$ and $31|F_{60}$.

((Leave Fibo))

Ex 103. Solve $x^2 + 6x - 3 \equiv 0 \text{ (mod 23)}$. $x = \frac{-6 \pm \sqrt{36 - 4(-3)}}{2} = \frac{-6 \pm \sqrt{48}}{2} = \frac{-6 \pm 2\sqrt{3}}{2} \equiv \frac{-6 \pm 5}{2}$

$\equiv \frac{-1}{2}, \frac{11}{2} \equiv \frac{22}{2}, \frac{12}{2} \equiv 11, 6 \text{ (mod 23)}$.

Solve $3x^2 + 2x - 3 \equiv 0 \text{ (mod 7)}$. $x = \frac{-2 \pm \sqrt{4 + 36}}{2} = \frac{-2 \pm \sqrt{40}}{2} = \frac{-2 \pm 2\sqrt{10}}{2}$. Now if $x \in \mathbb{Z}$ then $x \equiv 0, 1, 2, 3, 4, 5, 6 \text{ (mod 7)}$.

So $x^2 \equiv 0, 1, 4, 2, 2, 4, 1 \text{ (mod 7)}$. So no sol’n’s. End ex.

If $p$ odd prime, squares mod $p$ in set $\{1, \ldots, p - 1\}$ called quadratic residues mod $p$. Non-squares called quadratic non-residues.

<table>
<thead>
<tr>
<th>mod</th>
<th>quad res’s</th>
<th>quad non-res’s</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>5</td>
<td>1, 4</td>
<td>2, 3</td>
</tr>
<tr>
<td>7</td>
<td>1, 2, 4</td>
<td>3, 5, 6</td>
</tr>
<tr>
<td>11</td>
<td>1, 3, 4, 9, 10, 12</td>
<td>2, 6, 7, 8, 10</td>
</tr>
<tr>
<td>13</td>
<td>1, 3, 4, 9, 10, 12</td>
<td>2, 5, 6, 7, 8, 11</td>
</tr>
<tr>
<td>17</td>
<td>1, 2, 4, 8, 9, 13, 15, 16</td>
<td>3, 5, 6, 7, 10, 11, 12, 14</td>
</tr>
<tr>
<td>19</td>
<td>1, 4, 5, 6, 7, 9, 11, 16, 17</td>
<td>2, 3, 8, 10, 12, 13, 14, 15, 18</td>
</tr>
<tr>
<td>23</td>
<td>1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18</td>
<td>5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22</td>
</tr>
</tbody>
</table>

Thm 104 If $p$ an odd prime there are $\frac{p-1}{2}$ quadratic residues (squares) in $\mathbb{Z}_p^*$.

Pf. The map $s : \mathbb{Z}_p^* \rightarrow \mathbb{Z}_p^*$ by $s(x) = x^2$ is a hom since if $a, b \in \mathbb{Z}_p^*$ then $s(ab) = (ab)^2 = abab = aabb = a^2b^2 = s(a)s(b)$. The kernel is $\{x \in \mathbb{Z}_p^* \mid s(x) = 1\}$ if $x \in \ker$ then $x^2 = 1 \in \mathbb{Z}_p^*$ or $x^2 = 1 \equiv 0 \text{ (mod p)}$. Lag’s thm from last time implies $\exists \leq 2$ sol’n’s and clearly $\exists \geq 2$ sol’n’s so exactly two sol’n’s: $\pm 1$ (really 1, $p - 1$).

So now have onto hom $\mathbb{Z}_p^* @>s>> \mathbb{Z}_p^2 \subset \mathbb{Z}_p^*$ with kernel $\pm 1$. Thus $\mathbb{Z}_p^*/\{\pm 1\} \cong \mathbb{Z}_p^2$. Now $|\mathbb{Z}_p^*| = |\mathbb{Z}_p^*/\{\pm 1\}| = |\mathbb{Z}_p^2|/|\{\pm 1\}| = (p - 1)/2$. End pf.

When $-1$ a quad res? $p = 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97.$
When 2 a quad res? p = 7, 17, 23, 31, 47, 71, 73, 89, 97.
When −3 a quad res? p = 7, 13, 19, 31, 37, 43, 61, 67, 73, 79, 97.
When 3 a quad res? p = 11, 13, 23, 37, 47, 59, 61, 71, 73, 83, 97.

(Prove these later).

Ex. 104.5 Does \( x^2 \equiv 14 \pmod{55} \) have a solution? Well \( x^2 \equiv 14 \pmod{55} \) solvable \( \mathcal{CRT} \) \( x^2 \equiv 14 \equiv 4 \pmod{5} \) and \( x^2 \equiv 14 \equiv 3 \pmod{11} \) solvable.

Now \( x \equiv \pm 2 \pmod{5} \) and \( x \equiv \pm 5 \pmod{11} \) so 4 solutions mod 55.

Does \( x^2 \equiv 27 \pmod{55} \) have solution? No since \( x^2 \equiv 27 \equiv 2 \pmod{5} \) doesn’t. Enuf. End ex.

Let \( p \) be odd prime.
If \( p \mid n \) write \( \left( \frac{n}{p} \right) = 0 \).
If \( n \) is a quad res mod \( p \) write \( \left( \frac{n}{p} \right) = 1 \).
If \( n \) is a quad non-res mod \( p \) write \( \left( \frac{n}{p} \right) = -1 \).

\( \left( \frac{n}{p} \right) \) called Legendre symbol.

So \( \left( \frac{13}{23} \right) = 1, \left( \frac{14}{23} \right) = -1 \).

Thm (Euler). If \( p \) odd prime then \( \left( \frac{n}{p} \right) \equiv n^{\frac{p-1}{2}} \pmod{p} \).

Pf. Case 1. If \( n \equiv 0 \pmod{p} \) then \( n^{\frac{p-1}{2}} \equiv 0^{\frac{p-1}{2}} \equiv 0 = \left( \frac{n}{p} \right) \pmod{p} \).

Case 2. Assume \( \left( \frac{n}{p} \right) = 1 \). So \( n = x^2 \pmod{p} \) for some \( x \in \mathbb{Z}^*_p \). So \( n^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p} \).

Case 3. Example: \( \left( \frac{6}{11} \right) = -1 \).
\( 1 \cdot 6 \equiv 6 \pmod{11} \)
\( 2 \cdot 3 \equiv 6 \)
\( 4 \cdot 7 \equiv 6 \)
\( 5 \cdot 10 \equiv 6 \)
\( 8 \cdot 9 \equiv 6 \)

Get \( \frac{11-1}{2} = 5 \) distinct pairs with product 6. Could 7 show up in 2 different pairs? No, since \( 7x \equiv 6 \pmod{11} \) has uniq sol’n. Could 7 show up twice in some pair? No, since assume 6 not a square. Note \( 6^{\frac{11-1}{2}} \equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 10 \equiv -1 \pmod{11} \) by Wilson’s thm. Works for general \( n, p \) with \( \left( \frac{n}{p} \right) = -1 \). Proof is formalization of the above. End pf.

Cor 105. \( \left( \frac{-1}{p} \right) = 1 \) if \( p \equiv 1 \pmod{4} \).
\( \left( \frac{-1}{p} \right) = -1 \) if \( p \equiv 3 \pmod{4} \).

Cor 106. If \( p \) an odd prime, \( m, n \in \mathbb{Z} \) then \( \left( \frac{mn}{p} \right) = \left( \frac{m}{p} \right) \left( \frac{n}{p} \right) \).

Pf. \( \left( \frac{mn}{p} \right) \equiv (mn)^{\frac{p-1}{2}} \equiv m^{\frac{p-1}{2}} n^{\frac{p-1}{2}} \equiv \left( \frac{m}{p} \right) \left( \frac{n}{p} \right) \pmod{p} \). End pf.

To here twentieth lecture.

Ex 107. Compute \( \left( \frac{-30}{57} \right) = \left( \frac{-1}{57} \right) \left( \frac{3}{57} \right) \left( \frac{5}{57} \right) = 1 \cdot \left( \frac{3}{57} \right) \left( \frac{5}{57} \right) \). What’s \( \left( \frac{3}{57} \right) ? \left( \frac{5}{57} \right) ? \left( \frac{5}{57} \right) ? \) Have guesses from before. End ex.

Like to compute \( \left( \frac{2}{q} \right) \) where \( q \) also prime. Special for \( q = 2 \).
Thm (Gauss) Let \( p \) be an odd prime and \( (n,p) = 1 \). Let \( S \) be the set of least positive residues of \( \{n, 2n, \ldots, \frac{p-1}{2} \cdot n\} \mod p \). Let \( r \) denote the number of elements in \( S \) that are \( > \frac{p}{2} \). Then \( \left(\frac{2}{p}\right) = (-1)^r \).

Won’t prove.

Ex 108. \( p = 11, n = 6 \). Well \( \frac{p-1}{2} = 5 \). Have \( \{1 \cdot 6 = 6, 2 \cdot 6 = 12, 3 \cdot 6 = 11, 4 \cdot 6 = 24, 5 \cdot 6 = 30\} \). So \( S = \{6, 1, 7, 2, 8\} \). We have \( \frac{p}{2} = 5.5 \). So 3 of them \( (6, 7, 8) \) are \( > \frac{p}{2} \). So \( r = 3 \) and \( \left(\frac{6}{11}\right) = (-1)^3 = -1 \). End ex.

Prop 109. If \( p \) is an odd prime then

\[
\left(\frac{2}{p}\right) = \begin{cases} 
1 & \text{if } p \equiv \pm 1 \mod 8 \\
-1 & \text{if } p \equiv \pm 3 \mod 8 
\end{cases}
\]

Aside: Let \( m, n \in \mathbb{Z} \) with \( m \leq n \). The number of elements in \( \{2m, 2m + 2, 2m + 4, \ldots, 2n - 2, 2n\} \) is the same as in \( \{m, m + 1, m + 2, \ldots, n - 1, n\} \), which is \( n - m + 1 \).

Pf. Consider \( \{1 \cdot 2, 2 \cdot 2, 3 \cdot 2, \ldots, \frac{p-1}{2} \cdot 2 = p - 1\} \). All are own least residues.

If \( p = 8k + 1 \) then residues exceeding \( \frac{p}{2} = 4k + \frac{1}{2} \) and \( \leq p - 1 = 8k \) are \( \{4k + 2, 4k + 4, \ldots, 8k\} \). Set has size \( 4k - (2k + 1) + 1 = 2k \).

If \( p = 8k - 1 \) then residues exceeding \( \frac{p}{2} = 4k - \frac{1}{2} \) and \( \leq p - 1 = 8k - 2 \) are \( \{4k, 4k + 2, 4k + 4, \ldots, 8k - 2\} \). Set has size \( 4k - 1 - (2k) + 1 = 2k \).

In both cases, \( \left(\frac{2}{p}\right) = (-1)^{2k} = 1 \).

If \( p = 8k + 3 \) then residues exceeding \( \frac{p}{2} = 4k + \frac{3}{2} \) and \( \leq p - 1 = 8k + 2 \) are \( \{4k + 2, 4k + 4, \ldots, 8k + 2\} \). Set has size \( 4k + 1 - (2k + 1) + 1 = 2k + 1 \). So \( \left(\frac{2}{p}\right) = (-1)^{2k+1} = -1 \).

If \( p = 8k - 3 \) then residues exceeding \( \frac{p}{2} = 4k - \frac{3}{2} \) and \( \leq p - 1 = 8k - 4 \) are \( \{4k, 4k + 2, \ldots, 8k - 4\} \). Set has size \( 4k - 2 - (2k) + 1 = 2k - 1 \). So \( \left(\frac{2}{p}\right) = (-1)^{2k-1} = -1 \). End pf.

In Ex 107, like to compute \( \left(\frac{2}{p}\right) \) for an odd prime \( q \).

<table>
<thead>
<tr>
<th>(p)</th>
<th>3</th>
<th>5</th>
<th>7</th>
<th>11</th>
<th>13</th>
<th>17</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>0</td>
<td>-1</td>
<td>1</td>
<td>-1</td>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>5</td>
<td>-1</td>
<td>0</td>
<td>-1</td>
<td>1</td>
<td>-1</td>
<td>-1</td>
</tr>
<tr>
<td>7</td>
<td>-1</td>
<td>-1</td>
<td>0</td>
<td>1</td>
<td>-1</td>
<td>-1</td>
</tr>
<tr>
<td>11</td>
<td>1</td>
<td>1</td>
<td>-1</td>
<td>0</td>
<td>-1</td>
<td>-1</td>
</tr>
<tr>
<td>13</td>
<td>1</td>
<td>-1</td>
<td>-1</td>
<td>0</td>
<td>1</td>
<td>-1</td>
</tr>
<tr>
<td>17</td>
<td>-1</td>
<td>-1</td>
<td>-1</td>
<td>-1</td>
<td>-1</td>
<td>0</td>
</tr>
</tbody>
</table>

For which primes is row = col? OR Where does it lack symmetry? \( (3, 7), (3, 11), (7, 11) \).

If \( p \equiv 1 \mod 4 \) seems \( \left(\frac{2}{p}\right) = \left(\frac{q}{p}\right) \).

By sym, if \( q \equiv 1 \mod 4 \) seems \( \left(\frac{2}{q}\right) = \left(\frac{q}{p}\right) \).

If both \( p \equiv q \equiv 3 \mod 4 \) seems \( \left(\frac{2}{q}\right) = -\left(\frac{q}{p}\right) \).

Thm (The quadratic reciprocity law of Gauss). If \( p \) and \( q \) are distinct odd primes then \( \left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)} \).

Won’t prove. Legendre proved special cases before Gauss.

To here, twenty first lecture.

Recall \( \left(\frac{2}{p}\right) = 1 \) if \( q \) is a square mod \( p \) and \(-1\) if it’s not.

Thm (The quadratic reciprocity law of Gauss). If \( p \) and \( q \) are distinct odd primes then \( \left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)} \).
Cor 108. If \( p \) and \( q \) are distinct odd primes and either is \( 1 \pmod{4} \). Then \( (\frac{2}{p}) = (\frac{2}{q}) \). If both are \( 3 \pmod{4} \) then \( (\frac{2}{p}) = - (\frac{2}{q}) \).

Pf. WLOG let \( p \equiv 1 \pmod{4} \). Then \( 4 | p - 1 \) so \( \frac{p - 1}{2} \) is even. So \( ( -1)^{\frac{p-1}{2}} = 1 \). Thus \( (\frac{2}{p}) (\frac{2}{q}) = 1 \). Since both are \( \pm 1 \), they must be the same.

If \( p \equiv q \equiv 3 \pmod{4} \) then \( p - 1 = 4k + 2 \) and \( q - 1 = 4l + 2 \). So \( \frac{p - 1}{2} = 2k + 1 \) and \( \frac{q - 1}{2} = 2l + 1 \) are odd and \( ( -1)^{\frac{p-1}{2}} (\frac{2}{p}) (\frac{2}{q}) = -1 \). Thus \( (\frac{2}{p}) (\frac{2}{q}) = -1 \). Since both \( \pm 1 \), they are different. End pf.

((Ed, go to handout))

Ex 109. Evaluate \( x = (\frac{3321}{3607}) = (\frac{-286}{3607}) = (\frac{-1}{3607})(\frac{2}{3607})(\frac{143}{3607}) \).

Since \( 3607 \equiv 3 \pmod{4} \), \( (\frac{-1}{3607}) = -1 \).

Since \( 3607 \equiv 7 \equiv -1 \pmod{8} \), \( (\frac{2}{3607}) = 1 \).

Now \( 143 = 11 \cdot 13 \). So \( x = -1 \cdot 1 \cdot (\frac{11}{3607})(\frac{13}{3607}) \).

Now \( 13 \equiv 1 \pmod{4} \) and \( 3607 \equiv 11 \equiv 3 \pmod{4} \).

So \( x = -1 \cdot (\frac{11}{3607}) \cdot (\frac{13}{3607}) \).

Now \( 3607 \equiv 13 - 3 \equiv 10 \pmod{11} \) and \( 3607 \equiv 6 \pmod{13} \).

So \( x = (\frac{10}{11})(\frac{1}{11}) = (\frac{1}{11})(\frac{2}{11}) = -1 \cdot -1 \cdot (\frac{12}{11}) \) (since \( 11 \equiv 3 \pmod{4} \), \( 13 \equiv -3 \pmod{8} \) and \( 13 \equiv 1 \pmod{4} \)).

So \( x = (\frac{1}{11}) = 1 \).

The Legend symbol \( = 1 \) tells you that \( x^2 \equiv 3321 \pmod{3607} \) solvable. It doesn’t help find sol’n. Turns out \( 723^2 \equiv 3321 \pmod{3607} \).

Ex 109.3 Recall Cor 100: If \( p > 5 \) and \( x^2 \equiv 5 \pmod{p} \) has a sol’n then \( p | F_{p-1} \).

For which primes is \( 5 \) a quad residue? Want \( 1 = (\frac{5}{p}) = (\frac{5}{p}) \). For \( x \in \mathbb{Z} \), \( x \equiv 0, 1, 2, 3, 4(5) \) so \( x^2 \equiv 0, 1, 4, 4, 1(5) \). So for \( p \neq 5 \), \( p \) is a square/quad res mod 5 iff \( p \equiv 1, 4(\pmod{5}) \).

Prop 109.5 If \( p \equiv \pm 1 \pmod{5} \) then \( p | F_{p-1} \).

Ex. 109.7 Since \( 59 \equiv -1(\pmod{5}) \), we know \( 59 | F_{58} = 591286729879 = 59 \cdot 19489 \cdot 514229 \).

Ex 110. For which primes is \( -5 \) a quad residue (like 5.6 # 4, 5). Want \( 1 = (\frac{-5}{p}) = (\frac{-5}{p}) (\frac{5}{p}) \)

Case 1: \( p \equiv 1 \pmod{4} \). \( (\frac{-5}{p}) (\frac{5}{p}) = 1 \cdot (\frac{5}{p}) = 1 \) if \( p \equiv 1, 4 \pmod{5} \).

Case 2: \( p \equiv 3 \pmod{4} \). \( (\frac{-5}{p}) (\frac{5}{p}) = -1 \cdot (\frac{5}{p}) = -1 \) if \( p \equiv 2, 3 \pmod{5} \).

So \( (\frac{-5}{p}) = 1 \) if \( p \equiv 1, 9, 7, 3 \pmod{20} \).

End ex.

To here, twenty second lecture

Which integers are the sum of two squares? \( 1 = 1^2 + 0^2 \), \( 2 = 1^2 + 1^2 \), \( 4 = 2^2 + 0^2 \), \( 5 = 2^2 + 1^2 \), \( 8 = 2^2 + 2^2 \), \( 9 = 3^2 + 0^2 \), \( 10 = 3^2 + 1^2 \), \( 13 = 3^2 + 2^2 \), \( 16 = 4^2 + 0^2 \), \( 17 = 4^2 + 1^2 \), \( 18 = 3^2 + 3^2 \), \( 20 = 4^2 + 2^2 \), \( 25 = 5^2 + 0^2 \), \( 26 = 5^2 + 1^2 \), \( 29 = 5^2 + 2^2 \). For integer \( n \geq \mathbb{Z}_{\geq 1} \), can we write \( n = a^2 + b^2 \) for \( a, b \in \mathbb{Z} \).
Let $K = \mathbb{Z}, \mathbb{Q}$ or $\mathbb{R}$. Let $K[i] = \{a + bi \mid a, b \in K\}$. Define $N : K[i] \to K$ by $N(a + bi) = a^2 + b^2$. As in old homework can show that if $\alpha, \beta \in K[i]$ then $N(\alpha \beta) = N(\alpha)N(\beta)$.

Proposition 111. For all $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$, there exist, $\chi, \rho \in \mathbb{Z}[i]$ such that $\alpha = \chi \beta + \rho$ and $N(\rho) < N(\beta)$.

Ex 112. $(40-9i)\div(2+3i) = (do \ it) \ \frac{51}{34} + \frac{93}{134}i.$ Round each and get $4-11i$. We have $40-9i = (4-11i)(2+3i)+\rho$. So $\rho = (40-9i) - (4-11i)(2+3i) = -1 + i$. Note $N(-1+i) < N(2+3i)$. End ex.

Proof. Let $\alpha = a + bi, \ \beta = e + fi$ then $\frac{\alpha}{\beta} = \frac{a+bi}{e+fi} = \frac{ae+bf+(be-af)i}{e^2+f^2}$ is the nearest integers to $g$ and $h$. If half way in between, then round down.) Let $\chi = m + ni$ and $\rho = \alpha - \chi \beta.$ (Now show $N(\rho) < N(\beta)$.) We have $N(\rho) = N(\chi^2) \ (happened \ in \ \mathbb{Q}(i)) = N(\beta)N(\frac{a}{\beta}-\chi)$

$= N(\beta)(g+h-m-ni) = N(\beta)((g-m)+(h-n)i) = N(\beta)[(g-m)^2 + (h-n)^2] \leq N(\beta)(\frac{3}{2} + \frac{1}{2}) < N(\beta)$.

Note that using this proposition, we can define the Euclidean algorithm on $\mathbb{Z}[i]$ and greatest common divisors.

Ex. DON'T DO: Find gcd$(51-27i, 10-30i)$ in $\mathbb{Z}[i]$. $51 - 27i = (10-30i)(5) + 21 - 7i$. $10 - 30i = (2-1)(11 - 7i) + 2 + 6i$. $21 - 7i = -1 - 2i + (2+6i) + 1 + 3i$. $2 + 6i = 2$. So $2 + 6i = (2)(1+3i) + 0$. So gcd$(51 - 27i, 10 - 30i) = 1 + 3i$ or $(1 + 3i)(-i) = 3 - i$. End ex.

Assume $d \in \mathbb{Z}$. Let $\alpha, \beta \in \mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$. Note if $d = 1$ then $\mathbb{Z}[\sqrt{d}] = \mathbb{Z}$. We write $\alpha|\beta$ in $\mathbb{Z}[\sqrt{d}]$ if there is a $\gamma \in \mathbb{Z}[\sqrt{d}]$ such that $\beta = \alpha \gamma$. If $\alpha|1$ in $\mathbb{Z}[\sqrt{d}]$ we say $\alpha$ is a unit. Units in $\mathbb{Z}^\ast$? In HW, you'll show $\pm 1, \pm i$ are the only units in $\mathbb{Z}[i]$. If $u$ is a unit in $\mathbb{Z}[i]$ and $\alpha = u\beta$ then $\alpha$ and $\beta$ are associates. Note the associates of $2 + i$ are $2 + i, -1(2 + i) = -2 - i, i(2 + i) = -1 + 2i, -i(2 + i) = 1 - 2i$.

Let $\pi \in \mathbb{Z}[\sqrt{d}]$. We now say $\pi$ is a prime in $\mathbb{Z}[\sqrt{d}]$ if for all $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$, we have $\pi|\alpha \beta$ implies $\pi|\alpha$ or $\pi|\beta$.

If $\gamma \in \mathbb{Z}[\sqrt{d}]$, we say $\gamma$ is irreducible in $\mathbb{Z}[\sqrt{d}]$ if $\gamma = \alpha \beta$ with $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$ implies $\alpha$ or $\beta$ is a unit. (Note if one is a unit, the other is an associate of $\gamma$.)

Ex 113. In $\mathbb{Z}$ we talk about 5 being prime. But what about $-5$? In above definition, $-5$ is also prime. When we write $15 = (5)(3) = (-5)(-3),$ we don’t think of this as a violation of unique factorization because 5 and $-5$ are associates in $\mathbb{Z}$. We say that 5 and 5 are associated primes. Recall in $\mathbb{Z}[i]$, the units are $\pm 1, \pm i$. Note $5 = (2+i)(2-i).$ We will see soon that 2 + i is prime in $\mathbb{Z}[i]$. Then 2 + i, $-2 - i, -1 + 2i, 1 - 2i$ are associated primes. We'll show that 2 + i and 2 - i are not associated primes. So 2 - i, -2 + i, 1 + 2i, -1 - 2i are associated to each other and all different from the previous set of associates. So the following are, in a sense, equivalent factorizations of 5 = (2 + i)(2 - i) = (-2 - i)(-2 + i) = (1 + 2i)(1 - 2i) = (1 - 2i)(1 + 2i). For each such prime in $\mathbb{Z}[i]$ we will pick the ones of the form $a + bi$ where $a \geq b \geq 0$ as the standard representative among associates. End ex.

The greatest common divisor is defined up to unit multiple (i.e. associate). Again standardly pick $a + bi$ where $a \geq b \geq 0$.

Proposition 114. In $\mathbb{Z}[i]$, $\gamma$ is prime if and only if $\gamma$ is irreducible.

Proof ⇒ homework. ⇐ Let $\gamma \in \mathbb{Z}[i]$ be irreducible. Assume $\gamma|\alpha \beta$ with $\alpha, \beta \in \mathbb{Z}[i]$. ((Prove $\gamma|\alpha$ or $\gamma|\beta$)) Case 1. $\gamma|\alpha$. We’re done. Case 2. $\gamma$ does not $|\alpha$. Now gcd($\gamma, \alpha$) is a divisor of $\gamma$ so it is a unit $u$ or associate
u'γ of γ for some unit u' (u, u' ∈ ℤ[i]). If it’s an associate then u'γ|α so γ|α, a contradiction. So gcd(γ, α) is a unit, which we take to be 1. Since we have a Euclidean algorithm in ℤ[i], there is, ϵ ∈ ℤ[i] with ζγ + ϵα = 1. So ζγβ + ϵαβ = β. Since γ divides the left, then γ divides the right. End case 2. From the two cases, γ|α or γ|β. Thus γ is prime. End proof.

Going back, we see that our proof of the FTA for ℤ used only the fact that irreducibles are primes in ℤ. (In proof, replace p1 ≤ p2, by N(p1) ≤ N(p2), etc.) So we have a corresponding FTA for ℤ[i]. ((Want find primes in ℤ[i]))

Lemma 115. Let n ∈ ℤ and n|a + bi in ℤ[i] where a, b ∈ ℤ. Then n|a and n|b in ℤ. Proof. Note that \( \frac{a+bi}{n} = \frac{a}{n} + \frac{b}{n}i \) which is in ℤ[i] if an only if \( \frac{a}{n}, \frac{b}{n} \in ℤ \). End proof.

The notation p will always denote a prime in ℤ with p > 0.

Theorem 116. If p ≡ 1(mod 4) then p = x^2 + y^2 for some x, y ∈ ℤ.

PREPARE!!! Proof. Recall that if p ≡ 1(mod 4) then p = 4n + 1 for some n ∈ ℤ. Recall that \( |(2n)!|^2 \equiv (-1)(mod p) \) (5.4 #12). Let t = (2n)!. So p|t^2 + 1. This is also true in ℤ[i] so p|(t + i)(t – i) ∈ ℤ[i]. Assume that p is prime in ℤ[i]. Then p|t + i or p|t – i. Lemma 115 gives a contradiction. So p is not prime. So by Proposition 114, p is reducible. So there is a, β ∈ ℤ[i] such that p = αβ, and neither is a unit. Thus \( p^2 = N(p) = N(αβ) = N(α)N(β) \). So N(α)N(β) = p^2 in ℤ. Since N(α) and N(β) are positive, we have only two cases: \( \{N(α), N(β)\} \) are \( \{1, p^2\} \) or \( \{p, p\} \). If N(α) or N(β) = 1 then it is a unit, which is a contradiction. So N(α) = N(β) = p. If α = x + yi then N(α) = x^2 + y^2 = p. End proof.

We now want to determine the set of primes in ℤ[i].

Lemma 117. Let π be a prime in ℤ[i]. Then in ℤ[i] we have π|p for some prime p in ℤ. Proof. PREPARE!!! From homework (KK) \( N(a + bi) = (a + bi)(a – bi) = (a^2 + b^2) \). Let π ∈ ℤ[i] be prime. Then \( N(π) = π\overline{π} = m \) for some m ∈ ℤ. Now \( π\overline{π} = m = p_1^α_1 \cdots p_r^α_r \) (canonical factorization in ℤ). This still holds in ℤ[i], since \( π|p_1^α_1 \cdots p_r^α_r \) and π is prime in ℤ[i] then π divides one of the p_i’s. End proof.

Since primes of ℤ[i] divide primes of ℤ, to determine the primes of ℤ[i] we just have to factor primes of ℤ into primes of ℤ[i]. The primes of ℤ are 2, p ≡ 3(mod 4) and p ≡ 1(mod 4).

Lemma 118. The number 1 + i is prime in ℤ[i]. Proof. Note N(1 + i) = 2. From homework MM that makes 1 + i prime. End proof.

Note that \(-1(1 + i) = -1 – i, i(1 + i) = -1 + i, -i(1 + i) = 1 – i \) so all of these are associated primes. The factorization of 2 in ℤ[i] is \( 2 = (-i)(1 + i)^2 \) where 1 + i is prime and –i is a unit.

Lemma 119. Let p ≡ 3(mod 4). Then p is also prime in ℤ[i]. Proof: Assume p in not prime in ℤ[i]. Then p is reducible in ℤ[i]. so p = αβ in ℤ[i] where neither α nor β is a unit. So N(p) = p^2 = N(α)N(β). From homework JJ, γ is a unit if and only if N(γ) = 1. So N(α) = p and N(β) = p. Let α = a + bi then N(α) = a^2 + b^2 = p. From HW FF, primes of the form p ≡ 3(mod 4) can not be written as the sum of two squares. End proof.

Lemma 120. Let p ≡ 1(mod 4). Write p = a^2 + b^2 = (a + bi)(a – bi) with a, b ∈ ℤ. Then a + bi and a – bi are primes in ℤ[i]. Proof. Thin 116 gives the existence of a, b. Now N(a + bi) = N(a – bi) = p so a + bi and a – bi are prime from HW MM. End proof.

So for example, since \( 13 = 3^2 + 2^2 \) we have N(3 + 2i) = N(3 – 2i) = 13. So 3 + 2i and 3 – 2i are prime. We will soon show they are not associated. So \( 13 = (3 + 2i)(3 – 2i) \) and that is its factorization into primes.

Lemma 121. If a + bi is prime in ℤ[i] with N(a + bi) = p ≡ 1(mod 4) then i) a ≠ ±b, ii) a ≠ 0, iii) b ≠ 0.

Proof. i) If a = ±b then N(a + bi) = N(a ± ai) = 2a^2 ≠ p. ii) If a = 0 then N(bi) = b^2 ≠ p. iii) If b = 0 then N(a) = a^2 ≠ p. End proof.
Lemma 122. If \( a + bi \) is prime in \( \mathbb{Z}[i] \) with \( N(a + bi) = p \equiv 1 \pmod{4} \) then \( a + bi \) and \( a - bi \) are not associated primes. Proof. The associates of \( a + bi \) are \( a + bi, -a - bi, -b + ai, b - ai \). Now \( a + bi \not\equiv a + bi \pmod{2} \) since \( b \neq 0 \). \( a - bi \not\equiv -a - bi \pmod{2} \) since \( a \neq \pm b \). \( a - bi \not\equiv b - ai \pmod{2} \) since \( a \neq \pm b \).

Theorem 123. If \( \pi \) is a prime in \( \mathbb{Z}[i] \) then it is \( 1 + i, a \pm bi \) where \( N(a + bi) = a^2 + b^2 = p \equiv 1 \pmod{4} \) and \( a > 0 \) or \( p \in \mathbb{Z} \) with \( p \equiv 3 \pmod{4} \) or an associate of one of those. End Thm.

If \( a + bi \in \mathbb{Z}[i] \) then we can write \( a + bi = u\pi_1^{r_1} \cdots \pi_s^{r_s} \) where \( u \in \{ \pm 1, \pm i \} \) and the \( \pi \) are different primes as described in Thm 123. We will call this the canonical factorization of \( a + bi \) in \( \mathbb{Z}[i] \).

Corollary 124. Let \( a + bi \in \mathbb{Z}[i] \). Then the primes in \( \mathbb{Z}[i] \) dividing \( a + bi \) are the primes in \( \mathbb{Z}[i] \) that divide the primes in \( \mathbb{Z} \) dividing \( N(a + bi) \).

Example 125. Find the canonical factorization of \( 9 - 3i \). Note \( N(9 - 3i) = 92 = 3 \cdot 3 \cdot 2 \cdot 2 \). So \( 9 - 3i = u(1 + i)^2 \pi_1^{1} \pi_3^{1} \pi_5^{1} \cdot \pi_7^{1} \). We know that \( k = 1, l = 1, m + n = 1 \). Note \( \frac{9 - 3i}{2 + i} = \frac{21 - 3}{5} + \frac{3}{5}i \not\in \mathbb{Z}[i] \) and \( \frac{9 - 3i}{2 + i} = 3 - 3i \) so \( 2 + i \mid 9 - 3i \in \mathbb{Z}[i] \). Thus \( 9 - 3i = u(1 + i)^3(2 + i) \). Now \( 3 + 9i = -i(1 + i)(3 + 2i) \) is its canonical factorization.

Theorem 126. Let \( n \in \mathbb{Z}_{>0} \). Then \( n \) can be written as the sum of two squares if and only if the exponent of each prime that is \( 3 \pmod{4} \) dividing \( n \) is even.

Proof. \( \Rightarrow \): We know \( n = a^2 + b^2 \) with \( a, b \in \mathbb{Z} \) if and only if \( n = N(a + bi) \) for some \( a + bi \in \mathbb{Z}[i] \). Let \( a + bi \in \mathbb{Z}[i] \). Then we can uniquely write \( a + bi = u(1 + i)^m \pi_1^{r_1} \cdots \pi_s^{r_s} q_1^{s_1} \cdots q_r^{s_r} \) where \( u \) is a unit, each \( \pi \)'s is a different primes whose norm, \( p_j \), is a prime in \( \mathbb{Z} \) that is \( 1 \pmod{4} \) and the \( q_j \)'s are different primes in \( \mathbb{Z} \) that are \( 3 \pmod{4} \). We have \( N(a + bi) = 2^{m_0} p_1^{s_1} \cdots p_r^{s_r} q_1^{s_1} \cdots q_r^{s_r} \). Note that some of the \( p_j \)'s may be the same. This proves \( \Rightarrow \).

Assume \( n \in \mathbb{Z}_{>0} \) and \( n = 2^{m_0} p_1^{s_1} \cdots p_r^{s_r} q_1^{s_1} \cdots q_r^{s_r} \) with \( \prod p_k \equiv 1 \pmod{4} \) and \( q_k \equiv 3 \pmod{4} \) and each \( b_j \) is even. From Thm 116, for each \( p_j \) there are \( x_j, y_j \in \mathbb{Z} \) such that \( p_j = x_j^2 + y_j^2 \). Let \( (1 + i)^{m_0}(x_1 + y_1i) \cdots (x_r + y_r i)^{r_0} q_1^{s_1} \cdots q_r^{s_r} = a + bi \). Then \( a, b \in \mathbb{Z} \) and \( N(a) = n = a^2 + b^2 \). End proof.

For \( n \in \mathbb{Z}_{>0} \), let \( SS(n) \) denote the number of distinct representations of \( n \) as the sum of two squares. So \( SS(25) = 2 \) from \( 5^2 + 0^2 \) and \( 4^2 + 3^2 \) and \( SS(65) = 2 \) from \( 8^2 + 1^2 \) and \( 7^2 + 4^2 \). Representations of \( n \) as a sum of two squares come from \( n = a^2 + b^2 = N(a + bi) \). \( \pm a \pm bi \) and \( \pm b \pm ai \) are the only elements of \( \mathbb{Z}[i] \) giving the representation \( n = a^2 + b^2 \). These are exactly the associates and conjugates. So assoc’s and conj’s don’t increase the count of \( SS(n) \).

Example 127. Let \( n = 2^3 \cdot 5^1 \cdot 13^2 \cdot 31^0 \). Find \( SS(n) \). From Th’m 126, \( SS(n) \geq 1 \). If \( N(a + bi) = n \) then \( a + bi = u(1 + i)^3(2 + i)^2(2 - i)^2(3 + 2i)^3(3 - 2i)^2 \). The \( u \) does not affect \( SS(n) \). Ignoring \( u \), there are \( 4(4 + 1)(2 + 1) \) products. These all give different representations of \( n = a^2 + b^2 \) except the conjugates.

Focus on \((2 + i)^3(2 - i)^2\). The conjugates come in pairs unless an element is its own conjugate. That occurs just once with \((2 + i)^2(2 - i)^2(3 + 2i)^3(3 - 2i)^2 \). So of the \( 4(4 + 1)(2 + 1) \) products, one is its own conjugate. The others come in pairs. So \( SS(n) = 1 + \frac{(4 + 1)(2 + 1) - 1}{2} = \frac{(4 + 1)(2 + 1)}{2} + 1 \). In general, if \( n = 2^{m_0} p_1^{s_1} \cdots p_r^{s_r} q_1^{s_1} \cdots q_r^{s_r} \) is the canon repr’n with \( p_j \equiv 1 \pmod{4} \) and \( q_j \equiv 3 \pmod{4} \) and all \( a_j \) and \( b_j \) even then \( SS(n) = \frac{1}{2}(1 + \prod (a_i + 1) \).

Now let \( n = 2^3 \cdot 5^1 \cdot 13^2 \cdot 31^0 \). If \( N(a + bi) = n \) then \( a + bi = u(1 + i)^3(2 + i)^2(2 - i)^2(3 + 2i)^3(3 - 2i)^3 \). We have \( 4(4 + 1)(3 + 1) \) products. Again focus on \((2 + i)^2(2 - i)^2(3 + 2i)^3(3 - 2i)^2 \). Now no element is self conjugate because \( 3 \) is odd. In fact, if the \( b_j \)'s are even and at least one \( a_j \) is odd then \( SS(n) = \frac{1}{2}(a_i + 1) \).
Theorem 128. Assume $n \in \mathbb{Z}_{>0}$ and $n = 2^{m_z}p_1^{a_1} \cdots p_r^{a_r}q_1^{b_1} \cdots q_s^{b_s}$ with $p_k \equiv 1 \pmod{4}$ and $q_k \equiv 3 \pmod{4}$. If any $b_j$ is odd then $SS(n) = 0$. Assume all $b_j$'s are even. If any $a_j$ is odd then $SS(n) = \frac{1}{2} \prod (a_i + 1)$. If all $a_j$ are even then $SS(n) = \frac{1}{2} (1 + \prod (a_i + 1))$.

Review.

For which primes is $-2$ a quad residue?

If $a, b$ quadratic non-residues mod both $p$ and $q$, $p \neq q$, which equations have sol'ns? $x^2 \equiv a \pmod{p}$, $x^2 \equiv ab \pmod{p}$, $x^2 \equiv ab \pmod{q}$, $x^2 \equiv ab \pmod{pq}$, $x^2 \equiv a \pmod{pq}$.

What are last two digits of $2^{105}$?