Division: $d \mid \iff \exists c$ such that $a = cd$ **Upshot**: Any common divisor of a, b divides any linear combination of a, b

Euclid's Theorem: There are an infinite number of primes **Division Algorithm**: $a = bq + r$ for $0 \leq r < b$

Bezout's Identity: $\gcd(a, b) = ax + by$ **Upshot**: Any common divisor of a, b divides $\gcd(a, b)$

Euclidean Algorithm:

$$\begin{aligned} a &= q_1 b + r_1 \qquad 0 < r_1 < b \\ b &= q_2 b + r_2 \qquad 0 < r_2 < r_1 \\ &\cdots \\ r_{n-2} &= q_n r_{n-1} + 0 \end{aligned}$$

Mersenne Number: $2_n^n - 1$ n composite $\implies 2^n - 1$ composite

Fermat Number: $2^{2^n} + 1$ m not a power of 2 $\implies 2^m + 1$ is composite

2.13: Find all n such that $n^2 - n$ is prime

- $n^2 - n = n(n-1)$. One of these factors needs to be $1, -1 \implies n = -1, 2$

2.20: Suppose $a \mid b$ and $b \mid a$. Show that $a = \pm b$

- $a = bk \quad b = al \implies a = alk \implies lk = 1 \implies l = k = \pm 1 \implies a = \pm b$

2.25: Find all primes that can be written as a difference of squares. Same for fourth powers.

- $p = (a-b)(a+b) \implies a - b = 1 \implies a + b = 2b + 1$, which is an odd number. Thus p is an odd prime
- $p = (a^2 - b^2)(a+b) \implies (a-b) = (a+b) \implies a = 1, b = 0 \implies p = a^4 + b^4 = 1 \implies$ no primes

2.26: Show that $pn + 1 \leq p_1 p_2 \cdots p_n + 1$

- Let $N = p_1 p_2 \cdots p_n + 1$, then we have $p_{n+1} \leq p \leq N$ since no p_i divides N for $1 \leq i \leq n$

2.45: Find all n such that $n + 1 \mid n^2 + 1$

- Need $n + 1 \mid (n+1)(n-1) + 2 \implies n + 1 \mid 2 \implies n \in \{-3, -2, 0, 1\}$

2.46: Find all n such that $n + 1 \mid n^3 - 1$

- Need $n + 1 \mid n^3 + 1 - 2 \implies n + 1 \mid 2 \implies n \in \{-3, -2, 0, 1\}$

2.52: If $\gcd(a, b) = 1$, show that $\gcd(a + b, a - b) = 1$ or 2

- $\gcd(2a, 2b) = 2\gcd(a, b) \implies$. Any common divisor of $a + b, a - b$ divides $2a, 2b$

2.84: If $a^n - 1$ is prime, show that $a = 2$ and n is prime

- A factor of $a^n - 1$ is $a - 1 \implies a = 2$. By contraposition, suppose n is not prime, then $a^n - 1$ is not prime

2.85: If $a^n + 1$ is prime, show that $n = 2^k$

- BWOC, suppose $n = 2^k b$, then $(a^b + 1) \mid a^n + 1$. Contradiction

Linear Diophantine: $ax + by = c$ has a solution if and only if $\gcd(a, b) \mid c$ solutions: $x = x_0 + \frac{b}{d}t$ $y = y_0 - \frac{a}{d}t$

1. Verify $\gcd(a, b) \mid c$. If yes, divide by d, then $a'x + b'y = c'$ where $\gcd(a', b') = 1$
2. Use Extended Euclidean Algorithm to find solution $a'x + b'y = 1$ and multiply solution by c'
3. General solution is $(x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t)$

Note: No solutions to $ax + by = ab - a - b$ Always solutions to $n > ab - a - b$

Proposition: For a prime p, $p \mid ab \implies p \mid a$ or $p \mid b$

- Take $d = \gcd(a, p)$. If $d = a \implies p \mid a$. Otherwise $d = 1 \implies 1 = ax + py \implies b = abx + pby \implies p \mid b$

Unique Factorization Theorem: For any positive integer $n > 1$, it is prime or it can be written as a unique product of primes

- **Upshot**: $a \mid b \iff a_p \leq b_p$ for exponents
- **Upshot**: $\gcd(a, b)$ consists of exponents with $\min(a_p, b_p)$ and $\mathrm{lcm}(a, b)$ consists of exponents with $\max(a_p, b_p)$

4.8: Show that $\log_{10}(p)$ is irrational

- BWOC, suppose $\log_{10}(p) = \frac{a}{b} \implies p^b = 10^a = 2^a 5^a$. If $p = 2 \implies$ no factors of 5. If p is odd $\implies$ no factors of 2

4.11: Show that $a^n \mid b^n \implies a \mid b$. Show $a^m \mid b^n$ and $m \geq n \implies a \mid b$. Find example $a^m \mid b^n$ and $n > m$ and $a \nmid b$

- $a^n \mid b^n \implies na_i \leq nb_i \implies a_i \leq b_i \implies a \mid b$
- $a^m \mid b^n \implies ma_i \leq nb_i \implies a_i \leq b_i$ since $m \geq n \implies a \mid b$
- Let $a = 4, b = 6, m = 1, n = 2 \implies 4^1 \mid 6^2$ but $4 \nmid 6$

4.12: Show that $\gcd(a^n, b^n) = \gcd(a, b)^n$

- $\gcd(a, b)$ has exponents $\min(a_i, b_i) \implies \gcd(a^n, b^n)$ has exponents $n \min(a_i, b_i) \implies \gcd(a^n, b^n) = \gcd(a, b)^n$

4.17: Find p such that $3p + 1$ is a square. $5p + 1$ is a square. $29p + 1$ is a square

- $3p + 1 \implies 3p = (n + 1)(n - 1) \implies n - 1 = 3 \implies n = 4 \implies p = 5$
- $5p = (n + 1)(n - 1) \implies 5 = n - 1 \implies n = 6 \implies p = 6$ or $5 = n + 1 \implies n = 4 \implies p = 3$
- $29p = (n + 1)(n - 1) \implies 29 = n - 1 \implies n = 30 \implies p = 31$

Supplementary 8: Show that (p, q) are twin primes $\iff pq + 1$ is a square of an integer

- $\implies q = p + 2 \implies pq + 1 = p + 2p + 1 = (p + 1)^2$
- $\impliedby n^2 = pq + 1 \implies = pq = (n + 1)(n - 1)$ by UPF, $p = n - 1, q = n + 1$

Rational Root Theorem: All rational roots $\frac{u}{v}$ are of the form $u \mid a_0$ and $v \mid a_n$

Proposition: Odd square if $1 \pmod 8$ and even square is $0 \pmod 4$

Primitive Pythagorean Triple: $a^2 + b^2 = c^2$ where a, c are odd and b is even

- $a = n^2 - m^2 \qquad b = 2mn \qquad c = m^2 + n^2$ where m, n are relatively prime and one is odd and one is even

Proposition: Difference of Squares $\iff m$ is odd or $m \equiv 0 \pmod 4$

- Factor m into same parity factors $\implies x = \frac{u+v}{2} \qquad y = \frac{u-v}{2}$

Prime Factorizations of Factorials: $n! = p^b c$ and $p \nmid c \implies b = \lfloor \frac{n}{p} \rfloor + \lfloor \frac{n}{p} \rfloor + \cdots$

Riemann Zeta Function: $\zeta(s) = \sum_{=1}^{\infty} \frac{1}{n^s} = \prod (1 - p^{-1})^{-1}$

5.1.b: Find an integer n such that $n/2$ is a square, $n/3$ is a cube, $n/5$ is a fifth power

- $a - 1$ is even, $b - 1$ is a multiple of 3, $c - 1$ is a multiple of 5 $\implies a = 16, b = 10, c = 6$

Congruence: $a \equiv b \pmod m \iff m \mid a - b \iff a = b + km$

- $\gcd(c, m) = 1 \implies ac = bc \pmod m \implies a \equiv b \pmod m \qquad \gcd(c, m) = d \implies ac \equiv bc \pmod m \implies a \equiv b \pmod{\frac{m}{d}}$
- $x^2 \equiv 1 \pmod p \implies x \equiv \pm 1 \pmod p$

Divisibility Tests: $a \equiv a_0 \pmod{2, 5, 10} \qquad a \equiv \sum a_i \pmod{3, 9} \qquad a \equiv \sum (-1)^i a_i \pmod{11}$

Linear Congruence: $ax \equiv b \pmod m$ has a solution $\iff d = \gcd(a, b) \mid b \qquad$ comes from $ax - mk = b$

- Solutions are of the form $x = x_0 + \frac{m}{d} k$ for $0 \leq k \leq d$ and has d solutions
- **Upshot**: a has an inverse mod $m \iff \gcd(a, m) = 1$

Chinese Remainder Theorem: Let $m_1, \ldots, m_r$ be pairwise relatively prime, then the system $x \equiv a_i \pmod{m_i}$ has a unique solution x mod $m_1 \cdots m_r$

- Take the largest modulus and then plug into the other equations
- Can also be used to breakdown a congruence into a system of equation

  Example: $x^2 \equiv 1 \pmod{275 = 5^2 * 11}$ can be broken down into

$$x^2 \equiv 1 \pmod{25} \implies x \equiv 1, 24 \pmod{25}$$
$$x^2 \equiv 1 \pmod{11} \implies x \equiv 1, 10 \pmod{11}$$

Thus solutions are of the form

$$\begin{aligned}
x \equiv 1 \pmod{25} \quad & x \equiv 1 \pmod{11} \implies x \equiv 1 \pmod{275} \\
x \equiv 1 \pmod{25} \quad & x \equiv 10 \pmod{11} \implies x \equiv 76 \pmod{275} \\
x \equiv 24 \pmod{25} \quad & x \equiv 1 \pmod{11} \implies x \equiv 199 \pmod{275} \\
x \equiv 24 \pmod{25} \quad & x \equiv 10 \pmod{11} \implies x \equiv 274 \pmod{275}
\end{aligned}$$

Thus the solutions are $x \equiv \{1, 76, 199, 274\} \pmod{275}$

Fractions mod m: $\frac{a}{b} \pmod{m} = a(b^{-1}) \pmod{m}$ works if and only if $\gcd(b, m) = 1$

6.21d: If $a \equiv b \pmod{n}$ for every positive n, then $a = b$

- $a = bk$ and $b = al \implies a = alk \implies lk = 1 \implies a = b$

6.56: Solve $3x \equiv 8 \pmod{11}$ $\quad 6x \equiv 7 \pmod{9}$ $\quad 4x \equiv 12 \pmod{32}$

- $x \equiv 10 \pmod{11}$ $\quad$ No solution since $\gcd(6, 9) \nmid 7$ $\quad x \equiv 3 \pmod{8}$

6.69: Show that $x^2 - 2y^2 = 10$ has no integer solutions

- $x^2 \equiv 2y^2 \pmod{5} \implies x, y \equiv 0 \pmod{5}$ (by case analysis). Thus $x^2 - 2y^2 = 25k^2 - 50l^2 = 10 \implies$ no solutions

6.74: Solve the system $3x \equiv 2 \pmod{5}$ $\quad 4x \equiv 3 \pmod{7}$ $\quad x \equiv 2 \pmod{11}$

- $x = 4 + 11k \equiv 6 \pmod{7} \implies k \equiv 4 \pmod{7} \implies x = 4 + 11(4 + 7l) = 48 + 77l \equiv 4 \equiv \pmod{5} \implies l \equiv 3 \pmod{5}$

  Thus $x = 244 - 385m \implies x \equiv 244 \pmod{385}$

Proposition: $(x + y)^p \equiv x^p + y^p \pmod{p}$

Proposition: For $b \not\equiv 0 \pmod{p}, \{b, 2b, \ldots, (p-1)b\} \pmod{p}$ contains each unique class mod p

Fermat Theorem: $\forall b \in Z, b^p - b \equiv 0 \pmod{p}$ and $b \not\equiv 0 \pmod{p} \implies b^{p-1} \equiv 1 \pmod{p}$

- **Corollary**: $x \equiv y \pmod{p-1} \implies b^{\equiv} b^y \pmod{p}$
- **Fermat Prime Test**: For odd n and $b \not\equiv 0 \pmod{n}, b^{n-1} \not\equiv 1 \pmod{n} \implies n$ is NOT prime

Euler Phi Function: $\phi(n) = \prod_{i=1}^{r}(p_1^{a_i} - p_i^{a_i - 1}) = n \prod_{p|n}(1 - \frac{1}{p})$

Euler Theorem: For $\gcd(b, n) = 1$, $b^{\phi(n)} \equiv 1 \pmod{n}$

- **Corollary**: $x \equiv y \pmod{\phi(n)} \implies b^x \equiv b^y \pmod{n}$

Wilson Theorem: $(p-1)! \equiv -1 \pmod{p}$

- Pair inverses together and get left with $1(p-1) \equiv -1 \pmod{p}$
- **Corollary**: n is prime $\iff (n-1)! \equiv -1 \pmod{n}$

8.20: Show that $n^{17} - n \equiv 0 \pmod{510}$ for all integers n

- For all prime factors of n, we have that $n^{17} - n \equiv 0 \pmod{p} \implies n^{17} - n \equiv 0 \pmod{510}$ by unique factorization theorem

8.42: Show that $p \mid n \implies p - 1 \mid \phi(n)$. Show that there is no integer solutions to $\phi(n) = 26$

- Looking at the expansion of $\phi(n)$, we see that $p - 1 \mid \phi(n)$
- Divisors of 26 are $\{1, 2, 13, 26\}$ and thus possible prime divisors of n are $2, 3$ but there's no way to get a factor of 13

8.48: Prove or give a counterexample: $d \mid n \implies \phi(d) \mid \phi(n)$ $\quad \phi(d) \mid \phi(n) \implies d \mid n$ $\quad d \mid n \implies \phi(dn) = d\phi(n)$

- True: $p^{a_i} - p^{a_i - 1}$, we can pull out the necessary products from $\phi(n)$ to create $\phi(d) \implies \phi(d) \mid \phi(n)$
- False: $\phi(3) \mid \phi(4)$ but $3 \nmid 4$
- True: $\phi(dn)$ can extract a d factor out of this and the remaining still has $\phi(n)$

8.62: Let $n \neq 4$ be composite and show that $(n-1)! \equiv 0 \pmod{n}$

- $n = ab$. If $1 < a < b < n$, then $(n-1)!$ contains $a, b \implies n \mid (n-1)!$
- Otherwise $b = n/b \implies (n-1)!$ contains $b, 2b \implies b^2 = n \mid (n-1)$

8.63: Let $x = ((p-1)/2)!$, show that $-1 \equiv (-1)^{(p-1)/2}x^2 \pmod p$

- $(p-1)! = (1(p-1))(2(p-2))\cdots((p-1)/2))((p+1)/2) \implies -1$

Supplementary 14: Show that for odd n, $\phi(2n) = \phi(n)$ and for even n, $\phi(2n) = 2\phi(n)$

- $\phi(2n) = \phi(2)\phi(n) = \phi(n)$
- Let $n = 2^k m \implies \phi(2n) = \phi(2^{k+1})\phi(m) = 2^k\phi(m) = 2 * \phi(2^k)\phi(m) = 2\phi(n)$

Shift Cipher: $x \to x + k \pmod{26}$ **Affine Cipher**: $x \to ax + b \pmod{26}, \gcd(a, 26) = 1$

RSA Setup:

- Alice chooses $n = pq$ $\phi(n) = (p-1)(q-1)$ e such that $\gcd(e, \phi(n)) = 1$ d such that $ed \equiv 1 \pmod{\phi(n)}$
- Bob sends $c = m^e \pmod n$
- Alice decrypts $m = c^d \pmod n$

9.19: Alice uses (e_1, n) and (e_2, n) for RSA set up. Show that Eve can crack the message knowing m^{e_1} and m^{e_2}

- Eve can calculate $m^{e_1x+e_2y} \equiv m \pmod p$ since we can find x, y such that $e_1x + e_2y = 1$

9.23: Suppose Eve computes $c_1 \equiv 123^e c \pmod n$ and gives alice c_1 who decrypts it to m_1. How can Eve recover m from m_1?

- Eve calculates $(123^e c)^d \equiv m \pmod n$

Supplementary 26: For affine cipher $x \to ax + b \pmod 6$, prove that if b is odd, then no letter will be encrypted to itself

- BWOC, suppose that a letter encrypts to itself and suppose x is even, then b must be even. Contradiction

Order: $m = \text{ord}_n(a) \implies a^m \equiv 1 \pmod n$ Always exists since by Euler's Theorem, $a^{\phi(n)} \equiv 1 \pmod n$

Theorem: For $\gcd(a, n) = 1, a^k \equiv 1 \pmod n \iff \text{ord}_n(a) \mid k$

- $\implies$ Let $m = \text{ord}_n(a)$, then $k = qm + r \implies a^{qm+r} \equiv a^r \equiv 1 \pmod n \implies r = 0$. Thus $\text{ord}_n(a) \mid k$
- $\impliedby$ $a^{ml} \equiv 1 \pmod p$

Fermat Prime Proposition: $p \mid F_n \implies p \equiv 1 \pmod{2^{n+2}}$

Mersenne Prime Proposition: $q \mid M - n \implies q \equiv 1 \pmod p$

Primitive Root: $\text{ord}_p(g) = p - 1 \implies g$ is a **primitive root**

- $\gcd(g, p) = 1$ means that g is a primitive root $\iff$ every non-zero mod p is equivalent to a power of g mod p

Proposition: For primitive root g and odd p, $g^{(p-1)/2} \equiv -1 \pmod p$

- By Fermat, $g^{p-1} \equiv 1 \pmod p \implies g^{(p-1)/2} \equiv \pm \pmod p$. Cannot be the former because g is a primitive root

Proposition: For $m = \text{ord}_n(x), \text{ord}_n(x^i) = \frac{m}{\gcd(i,m)}$

- **Corollary**: For a primitive root \$$g$, we have that $\text{ord}_p(g^i) = \frac{p-1}{\gcd(i,p-1)}$
- **Corollary**: Primitive roots are congruent to $g^i \pmod p$ for $\gcd(i, p-1) = 1$
- **Corollary**: There are $\phi(p-1)$ primitive roots for a prime p

Proposition: For $h \not\equiv 0 \pmod p$, h is a primitive root for p is equivalent to for $q \mid p - 1, h^{(p-1)/q} \not\equiv 1 \pmod p$

Discrete Log Problem: Find x such that $g^x \equiv 1 \pmod p$ solved using **Baby-step Giant-step Method**

- Let $N = \lceil\sqrt{p-1}\rceil$ and create lists $g^i \pmod p$ and $hg^{-Nj} \pmod p$ for $0 \le i, j \le N - 1$
- $g^i \equiv hg^{-Nj} \pmod p \implies x = i + Nj$

11.31: Let $p \equiv 1 \pmod 8$ be prime and g be a primitive root. Let $y \equiv g^{(p-1)/8} \pmod p$. Show that $y^4 \equiv -1 \pmod p$ and $x \equiv y + y^{-1} \implies x^2 \equiv 2 \pmod p$

- $y^4 \equiv g^{(p-1)/2} \equiv -1 \pmod p$
- $x^2 \equiv y^2 + y^{-2} + 2 \equiv g^{(p-1)/4}(1 + g^{(p-1)/2}) + 2 \equiv 2 \pmod p$

11.46: Suppose that $7^{57} \equiv 11 \pmod{101}$ and $2^9 \equiv 7 \pmod{101}$. Solve $2^x \equiv 11 \pmod{101}$ and solve $7^y \equiv 2 \pmod{101}$

- $(2^9)^{57} \equiv 2^{513} \equiv 2^{13} \pmod{101} \implies x = 13$
- $7^y \equiv 2^{9y} \equiv 2 \pmod{100} \implies 9y \equiv 1 \pmod{100} \implies y = 89$

11.49: Let g be a primitive root for an odd prime p. Suppose $g^x \equiv h \pmod{p}$. Show that $h^{(p-1)/2} \equiv 1 \implies x$ is even and $h^{(p-1)/2} \equiv -1 \implies x$ is odd

- $g^x \equiv h^{x(p-1)/2} \equiv 1 \pmod{p} \implies p-1 \mid x(p-1)/2 \implies x$ is even
- $g^x \equiv h^{x(p-1)/2} \equiv -1 \pmod{p}$ and $g^{(p-1)/2} \equiv -1 \pmod{p} \implies g^{(x-1)(p-1)/2} \equiv 1 \pmod{p}$

  This only happens when $p-1 \mid (x-1)(p-1)/2 \implies x-1$ is even $\implies x$ is odd

Supplementary 30: Let p be a prime number. Prove that F_p is prime $\iff \text{ord}_p(a)$ is a power of 2 for every $a \not\equiv 0 \pmod{n}$

- $\implies$ Let $p = 2^{2^n} + 1$ and let g be a primitive root, so $\text{ord}_p(g) = p - 1 = 2^{2^n}$

  Every integer $a \not\equiv 0 \pmod{p}$ is a power of g mod p so $a \equiv g^i \implies \text{ord}_p(g^i) = \frac{p-1}{\gcd(i,p-1)}$

  Thus the order must be some power of 2

Quadratic Residue: a is a square mod n

Proposition: For odd prime and $a \not\equiv 0 \pmod{p}$, $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$ and a is a QR $\iff a^{(p-1)/2} \equiv 1 \pmod{p}$

- First statement holds from Fermat Theorem
- $\implies$ Let $x^2 \equiv a \pmod{p} \implies x^{p-1} \equiv a^{(p-1)/2} \equiv 1 \pmod{p}$
- $\impliedby$ Take a primitive root $g^i \equiv 1 \implies 1 \equiv g^{i(p-1)/2} \implies p-1 \mid i(p-1)/2 \implies a \equiv g^i \equiv (g^k)^2$

Legendre Symbol: $(\frac{a}{p}) = \begin{cases} +1 & x^2 \equiv 1a \pmod{p} \\ -1 & x^2 \not\equiv a \pmod{p} \end{cases}$

- $(\frac{a}{p}) \equiv a^{(p-1)/2} \pmod{p}$
- $(\frac{a}{p})(\frac{b}{p}) = (\frac{ab}{p})$
- $a \equiv b \pmod{p} \iff (\frac{a}{p}) = (\frac{b}{p})$
- $(\frac{-1}{p}) = \begin{cases} +1 & p \equiv 1 \pmod{4} \\ -1 & p \equiv 3 \pmod{4} \end{cases}$
- $(\frac{q}{p}) = \begin{cases} (\frac{p}{q}) & p \equiv 1 \pmod{4} \vee q \equiv 1 \pmod{4} \\ -(\frac{p}{1}) & p \equiv q \equiv 3 \pmod{4} \end{cases}$
- $(\frac{2}{p}) = \begin{cases} +1 & p \equiv \pm 1 \pmod{8} \\ -1 & p \equiv \pm 3 \pmod{8} \end{cases}$

Proposition: For $p \equiv 3 \pmod{4}$, one of $x, -x$ is a Quadratic Residue and $y \equiv x^{(p+1)/4} \implies y^2 \equiv \pm x \pmod{p}$

- $(\frac{-x}{p}) = -(\frac{x}{p}) \implies y^2 \equiv x^{(p-1)/2}x = \pm(x)$

Proposition: Quadratic solution $\iff b^2 - 4ac$ is a Quadratic Residue

13.11: For $p \equiv q \pmod{5}$ show that $(\frac{5}{p}) = (\frac{5}{q})$

- $(\frac{5}{p}) = (\frac{p}{5}) = (\frac{q}{5}) = (\frac{5}{q})$

13.18: Let p be a prime $p \equiv 3 \pmod{4}$ and suppose $q = 2p + 1$ is also prime. Show that 2 is a QR mod q and $2^p \equiv 1 \pmod{q}$

- $(\frac{2}{q}) = +1$ since $q \equiv -1 \pmod{8}$
- Since we know there is an x such that $x^2 \equiv 2 \implies x^{2p} \equiv 1 \pmod{q} \equiv 2^p$

13.22: Let p be an odd prime such that $2^p - 1$ is prime. Show that $(\frac{3}{2^{p-1}}) = -1$

- Note that $2^p - 1 \equiv 3 \pmod{4}$ and that $2^p = 2 * 4^{(p-1)/2} \equiv 2 \pmod{3} \implies 2^p - 1 \equiv 1 \pmod{3}$

  Thus $(\frac{3}{2^{p-1}}) = -(\frac{2^p-1}{3}) = -(\frac{1}{3}) = -1$

13.24: Prove that there are infinitely many primes $p \equiv 3 \pmod 8$

- Let $N = (p_1 \cdots p_n)$ and $M = N^2 + 2$. Clearly no $p_i \mid M$ so take q to be a prime factor of $M \implies N^2 \equiv -2 \pmod q \implies$ only has solution if $q \equiv 1 \pmod 8$ or $q \equiv 3 \pmod 8$

  Furthermore, $N \equiv 3^n \implies N^2 \equiv 9^n \equiv 1 \pmod 8$

  Thus $M \equiv 3 \pmod 8$. Thus M must have at least one prime divisor of the form $r \equiv 3 \pmod 8$ not in the list above. Contradiction

13.25: Show that ther eare infinitely many primes $p \equiv 7 \pmod 8$

- Let $N = (p_1 \cdots p_n)$ and $M = N^2 - 2$. Clearly no $p_i \mid M$ so take q to be a prime factor of $M \implies N^2 \equiv 2 \pmod q \implies$ only has solutions if $q \equiv \pm 1 \pmod 8$

  Furthermore $N \equiv 7^n \implies N^2 \equiv 1 \pmod 8$

  Thus $M \equiv 7 \pmod 8$. Thus M must have at least one prime divisor of the form $r \equiv 7 \pmod 8$ not in the list above. Contradiction

13.29: Solve $y^2 \equiv 2 \pmod{23}$

- $y^2 \equiv \pm x$ and $y = x^{(p+1)/2} \implies 2^{(23+1)/4} \equiv 18 \pmod{23}$

Diffie-Hellman:

1. Alice and Bob agree on a prime p and a primitive root g
2. Alice chooses secret a and sends $h_1 \equiv g^a \pmod p$ and Bob chooses secret b and sends $h_2 \equiv g^b \pmod p$
3. Alice computes $k \equiv h_2^a$ and Bob computes $k \equiv h_1^b$. This is the shared key $k \equiv g^{an}$
4. Eve can intercept g, g^a, g^b. If DLP is easy, then Eve can use g, g^a to find a and then compute $k = g^{ba}$

Perfect Number: $n = \sum_{d|n, d \neq n} d$ **Abundant** $n >$ **Deficient** $n <$

- $\sigma(n) = \sum_{d|n} d \implies$ Perfect if and only if $n = \sigma(n) = n \implies \sigma(n) = 2n$

Proposition: $\sigma(p^k) = 1 + p + \cdots + p^k = \frac{p^{k+1}}{p-1}$

Theorem: Let n be an even perfect number, then there exists a unique prime such that 2^{p-1} is prime and $n = 2^{p-1}(2^p - 1)$

Multiplicative Function: $f(mn) = f(m)f(n)$ for all $\gcd(m,n) = 1$

Proposition: If $f(p^j) = g(p^j)$ for all primes, then $f(n) = g(n)$

- $f(n) = f(p_1^{a_1})f(p_2^{a_2}) \cdots f(p_r^{a_r}) = f(p_1^{a_1})f(p_2^{a_2}) \cdots f(p_r^{a_r}) = g(n)$

Lemma: For $\gcd(m,n) = 1$ and divisor d of mn, d has a unique decomposition $d = d_1 d_2$ where $d_1 \mid m$ and $d_2 \mid n$

- By unique prime factorization, $d_1 = p_1^{a_1'} \cdots p_r^{a_r'}$ $d_2 = q_1^{b_1'} \cdots q_s^{b_s'} \implies d = d_1 d_2$ where $d_1 \mid m$ and $d_2 \mid n$

Proposition: $g(n) = \sum_{d|n} f(d)$ is multiplicative

16.12a: Show that the last digit of an even perfect number is always 6 or 8

- $n = 2^{p-1}(2^p - 1)$. Looking at powers of $2^{k \pmod 4} \pmod{10}$, we have that $\{(1,2),(2,4),(3,8),(4,6)\} \implies 2^{p-1}(2^p - 1)$ is $\equiv 6, 8 \pmod{10}$

16.14a: Show that $\tau(n)$ is odd if and only if n is a square

- $\implies \tau(n) = (a_1 + 1) \cdots (a_m + 1)$ is a product of odd numbers. Thus each a_i is even $\implies n$ is a square
- $\impliedby$ All exponents in the prime factorization of n is even. Thus $\tau(n)$ is odd

Supplementary 33: Evaluate $\tau(1440)$ and $\sigma(1440)$

- $1440 = 2^5 * 3^2 * 5 \implies \tau(1440) = 6 * 3 * 2 = 36$ $\sigma(1440) = (2^6 - 1)(\frac{3^3-1}{2})(\frac{5^2-1}{4})$

Gaussian Integer: $Z[i] = \{a + bi \mid a, b \in Z\}$ $\|a + bi\| = \sqrt{a^2 + b^2}$ $N(a + bi) = a^2 + b^2$

Theorem: The following are equivalent

- $N(\alpha) = 1$ $1/\alpha \in Z[i]$ $\alpha = \pm 1$ or $\alpha = \pm i$

Units: $\pm 1, \pm i$ **Irreducibles**: α is not a unit and $\alpha = \beta\gamma \implies \beta$ or γ are units

- $1+i$ $\quad p \equiv 3 \pmod 4$ $\quad (a+bi)(a-bi)$ where $a^2+b^2 = p \equiv 1 \pmod 4$

Proposition: $N(\alpha) = p \implies \alpha$ is irreducible

- $\alpha = \beta\gamma \implies N(\beta) = 1$ or $N(\gamma) = 1$
- **Proposition**: $p \equiv 3 \pmod 4 \implies p$ is irreducible
- $p = \beta\gamma \implies p^2 = N(\gamma)N(\beta)$. BWOC suppose $N(\gamma) = p \implies a^2+b^2 = p \equiv 3 \pmod 4$. Impossible

Division Algorithm: $\alpha = \beta\eta + \rho$ $\quad 0 \leq N(\rho) < N(\beta)$

- **Divides**: $\alpha \mid \beta$ if and only if $\beta = \alpha\gamma$

Theorem: The following are equivalent

- $\gamma = \gcd(\alpha, \beta)$ exists $\quad \gamma'$ is another gcd $\implies \gamma'$ is an associate of γ $\quad \exists x, y$ such that $\gamma = \alpha x + \beta y$
- $\sigma \mid \alpha, \beta \implies N(\sigma) \leq N(\gamma)$ $\quad \sigma \mid \alpha, \beta)$ and $N(\sigma) = N(\gamma) \implies \sigma$ is a gcd

Proposition: For irreducible π, $\pi \mid \alpha\beta \implies \pi \mid \alpha$ or $\pi \mid beta$

- Let $\gamma = \gcd(\pi, \alpha)$. If $\gamma = \pi \implies$ done
- Otherwise let $\gamma = \alpha \implies \pi$ not reducible contradiction. Thus $\gamma = 1 \implies \beta = \alpha\beta x + \pi\beta x \implies \pi \mid \beta$
- **Corollary**: Proposition holds for $\pi \mid \alpha_1\alpha_2\cdots\alpha_n$ for relatively pairwise prime α_i, α_j

Unique Prime Factorization Theorem: Every $\alpha \in Z[i]$ is a unit, irreducible, or product of irreducibles where factorization is unique up to order of factors and multiplication by units

- Proof involves picking α with minimal norm $N(\alpha)$