ChatGPT summaries:

- $\text{ord}_n r = \varphi(n) \iff r$ is a primitive root mod n
  $\text{ord}_7 2 = 3$ because $2^3 \equiv 1 \pmod 7$
- $\text{ord}_n a = t \Rightarrow \text{ord}_n(a^u) = \frac{t}{\gcd(t,u)}$
- every prime has one primitive root, usually more $(1, 2, p-1)$ relatively prime
- p^2, p prime, odd: $p=7$, primitive root is 3, so primitive root of p^2 must be 3 or 10 (it's 3 so 49, 343, 2401, ... too)
- p is odd prime $\& t \in \mathbb{Z}$, then $2^p t$ has primitive root

$3^1 \equiv 3 \pmod 7$ $3^2 \equiv 2$ $3^3 \equiv 6$ $3^4 \equiv 4$ $3^5 \equiv 5$ $3^6 \equiv 1$
$\text{ind}_3 1 = 6$ $\text{ind}_3 2 = 2$ $\text{ind}_3 3 = 1 \ldots$

$y^2 \equiv x^3 - 2 \pmod 7$
$1^3 - 2 = -1$ ✗ $2^3 - 2 = 6$ ✗ $3^3 - 2 = 25$ ✓ $4^3 - 2 = 62$ ✗ $5^3 - 2 = 123$ ✓
$6^3 - 2 = 214$ ✓
✱ $(3,2), (3,-2), (5,2), (5,-2), (6,2), (6,-2)$

Sum of $(3,2) + (5,5)$:

$\frac{5-2}{5-3} = 3/2$ $m = 3 \cdot 2^{-1}$ $2 \cdot \boxed{4} \equiv 8 \pmod 7 \equiv 1$
$m \equiv 3 \cdot 4 \pmod 7 \equiv 5$

$x_3 = m^2 - x_1 - x_2$
$y_3 = m(x_1 - x_3) - y_1$

$x_3 = 5^2 - 3 - 5 \pmod 7 \equiv 3$ $\boxed{(3,5)}$
$y_3 \equiv 5(3-3) - 2 \equiv -2 \pmod 7 \equiv 5$

Sum of $(3,2) + (3,2)$: $P_1 + P_2 = P_3(x_3, y_3)$
$P_1 = P_2 \Rightarrow m \equiv (3x_1^2 + b)(2 \cdot y_1)^{-1}$ $(27+b)(2 \cdot 2 \pmod 7)^{-1}$
$\equiv 6 * 4^{-1} \equiv 6 \cdot 2 \pmod 7 \equiv 5$

$x_3 \equiv 5^2 - 3 - 3 \pmod 7 \equiv 5$ $\boxed{(5,2)}$
$y_3 \equiv 5(3-5) - 2 \equiv -12 \pmod 7 \equiv -5 \equiv 2$

ElGamal Encryption:

Gen

$q \in \mathbb{P} \rightarrow g \in \mathbb{Z}_q^*$ · $s_0 \in \{2, \ldots, q-2\}$

$P_0 = g^{s_0} \bmod q$

$PK: q, g, P_0$ →

$SK: q, s_0$

ENC

$m \in \mathbb{Z}_q^*$

$s_1 \in \{2, \ldots, q-2\}$

$P_1 = g^{s_1} \bmod q$

$K = P_0^{s_1} \bmod q$

$c(m) = mK \bmod q$

← $CT: C, P_1$

DEC

$K = P_1^{s_0} \bmod q$

$m(c) = cK^{-1} \bmod q$

$K = P_1^{s_0} = (g^{s_1})^{s_0} = g^{s_1 s_0} = g^{s_0 s_1} = (g^{s_0})^{s_1} = P_0^{s_1} \bmod q$

log problem

$s_0 = \log_g P_0 \bmod q$ $\quad$ $s_1 = \log_g P_1 \bmod q$

Perfect numbers and mersenne

$n = 2^{m-1}(2^m - 1)$ where $m \geq 2$ & $2^m - 1$ is prime

* If m is a positive integer and $2^m - 1$ is prime, then m must be prime.

* If p is an odd prime, then any divisor of the mersenne prime is of the form $2kp + 1$

* Lucas-Lehmer test: Let p be prime and let $M_p = 2^p - 1$
$r_k \equiv r_{k-1}^2 - 2 \pmod{M_p}$
M_p is prime iaof $r_{p-1} \equiv 0 \pmod{M_p}$

$M_5 = 2^5 - 1 = 31$ $r_1 = 4$ $r_2 = 4^2 - 2 \equiv 14 \pmod{31}$ $r_3 \equiv 14^2 - 2 \equiv 8 \pmod{31}$
$r_4 \equiv 8^2 - 2 \equiv 0 \pmod{31}$

Cryptology

decryption/deciphering
plaintext ⟷ ciphertext
encryption/enciphering

$C \equiv P + 3 \pmod{26}$, $0 \leq C \leq 25$

	0	1	2	3
Plain	A	B	C	D
Cipher	D	E	F	G

$C \equiv 7P + 10 \pmod{26}$

1	2	3	4
A	B	C	D
K	R	Y	F
10	17	24	5

Public Key Cryptography

- private key cryptosystems (shift cipher, affine cipher)

RSA

Encryption: $C \equiv P^e \pmod n$ * public key (e, n)
Decryption: $P \equiv C^d \pmod n$ * private key (d, n)

$n = p \cdot q$ (p, q large primes)
$e > (p-1)$ & $e > (q-1)$ $\gcd(e, (p-1)(q-1)) = 1$
* d is modular inverse of $e \pmod{(p-1)(q-1)}$
$(de) \pmod{(p-1)(q-1)} \equiv 1 \pmod{(p-1)(q-1)}$

ex $n = 11 \cdot 13 = 143$ $(p-1)(q-1) = 120$ plaintext = 7

$e = 11$ encryption $(11, 143)$; $d = 11$ decryption $(11, 143)$
$C = 7^{11} \pmod{143} \equiv 106 \pmod{143}$; $D = 106^{11} \pmod{143} \equiv 7 \pmod{143}$

Diffie Hellman / Poker / secret sharing

- Two public numbers (p - large prime, r - primitive root mod p)
- Alice and Bob choose numbers between 1 and p-2 (k_1, k_2)
- $Y_1 = r^{k_1} \pmod p$, $Y_2 = r^{k_2} \pmod p$
- $K = Y_2^{k_1} = Y_1^{k_2}$

ex $p = 23, r = 5, k_1 = 6, k_2 = 15$ $Y_1 = 5^6 \pmod{23} \equiv 8$ (6: private, 8: public), $Y_2 = 5^{15} \pmod{23} \equiv 19$ (15: private, 19: public)
$K = 19^6 \pmod{23} \equiv 8^{15} \pmod{23} \equiv 2$

Poker

$(Q\spadesuit)^{K} \bmod P$ ← Ron's key $\qquad (Q\spadesuit)^{J} \bmod P$ ← John's key

$((Q^J)^K)^{K^{-1}} = Q^J \bmod p \qquad (Q^J)^{J^{-1}} \Rightarrow Q\spadesuit$

$Q^{11} = Q \cdot (Q^5)^2 \qquad Q^5 = Q \cdot (Q^2)^2 \qquad Q^2 = Q \cdot Q$

Secret sharing

key K with $k_1, k_2, \ldots k_r$ shadows, $s < r$

$m_1 < m_2, m_3 \ldots$

ex $K = 4$, $(2, 3)$ with $p = 7, m_1 = 11, m_2 = 12, m_3 = 17$

$M = m_1 \cdot m_2 = 132 > p m_3 = 119$

we pick $t = 14 < M/p = 132/17$ (and)

$k_0 = K + tp = 4 + 14 \cdot 7 = 102$

$k_1 \equiv 102 \equiv 3 \pmod{11}$

$k_2 \equiv 102 \equiv 6 \pmod{12}$

$k_3 \equiv 102 \equiv 0 \pmod{17}$

We can recover K with any 2 shadows

Suppose we know $k_1 = 3$ & $k_3 = 0$

$m_1 m_3 = 11 \cdot 17 = 187$

$k_0 \equiv 102 \pmod{187}$ because $0 \leq k_0 < M = 132 < 187$,

we know $k_0 = 102 \Rightarrow K = k_0 - tp = 102 - 14 \cdot 7 = 4$

Final Questions:

$(3+1)! + 2$

$(3+1) + 3$

$(3-1)! + 4$

Suppose $n \in \mathbb{N}$ is arbitrary. We want to show there exists n consecutive composite integers, and thus there exist arbitrarily large gaps between primes in $\mathbb{N}$. Suppose we have a sequence $(n+1)! + 2, (n+1!) + 3, \ldots, (n+1)! + (n+1)$; each number in the sequence must be composite because $(n+1)! + 2$ can be written as $2k + 2$, $k \in \mathbb{N}$, and $2 \mid 2(k+1)$. Likewise, $(n+1)! + 3$ can be written as $3k + 3$, $k \in \mathbb{N}$, and $3 \mid 3(k+1)$. This follows up to $(n+1)! + (n+1)$ because $n+1 \mid (n+1)!$. Therefore, the sequence $(n+1)! + 2, (n+1\text{?})! + 3, \ldots, (n+1)! + (n+1)$ contains n consecutive composite integers. Then it follows that if we have an arbitrarily large $n \in \mathbb{N}$, ~~there will be an error~~ we can construct a sequence with an arbitrarily large amount of consecutive composite integers, and thus there must be an arbitrarily large gap ~~between two~~ successive primes.

$\frac{-6}{2}$ $-\frac{3}{1}$ -3

$-\frac{5}{4} \pmod{11}$ $1 \cdot 1 \equiv 1 \pmod{11}$ $4 \cdot 3 \equiv 1 \pmod{11}$

$1 \cdot -6 \equiv 5 \pmod{11}$

$-5 \pmod{11} \equiv 6$

$6 \cdot 3 \equiv 7 \pmod{11}$

$y = 7x + 8 \pmod{11}$

$-\frac{20}{55} \pmod{11}$

$\frac{3}{5} \cdot \frac{4}{2} \equiv 1 \pmod{11}$

$4 \cdot 10 \equiv 7 \pmod{11}$

$5x+9$

Let $n \in \mathbb{Z}$ be arbitrary and suppose we have two integers n & $n+1$. we want to prove $\gcd(n, n+1) = 1$. BWOC suppose $\gcd(n, n+1) = k$, $k \in \mathbb{N}$ & $k > 1$. Then it follows that $k \mid n$ & $k \mid n+1$. By properties of divisibility, then k must divide the difference of n & $n+1$. Thus, $k \mid (n+1) - n \Rightarrow k \mid 1$. This is a contradiction because k can only be 1, but we've already said $k > 1$. Therefore our original claim holds, and $\forall n \in \mathbb{Z}$, $\gcd(n, n+1) = 1$.

Quizzes:

ex $m = 9$, since $\gcd(4, 9) = 1$ we know $4 \in \mathbb{Z}_9^*$. Find order of 4 in group $\mathbb{Z}_9^*$

By Euler's Totient Function: $\varphi(9) = 9 * (1 - \frac{1}{3}) = 6$ $|1, 2, 4, 5, 7, 8| = 6$

Verifying $4 \in \mathbb{Z}_9^*$. Now do powers of 4 (mod 9) until $4^k \equiv 1 \pmod{9}$

$4^1 \equiv 4 \pmod{9}$, $4^2 \equiv 7 \pmod{9}$, $4^3 \equiv 1 \pmod{9}$, thus order is 3.

ex 19 14 3 encrypted using RSA with public key $n = 118$ $e = 39$ (A = 10, B = 11 ...)

$118 = 59 \cdot 2$ $58 \cdot 1 = 58$ $\boxed{3} * 39 \equiv 1 \pmod{58}$

$19^3 \pmod{118} \equiv 15$, $14^3 \pmod{118} \equiv 30$ $3^3 \pmod{118} \equiv 27$

FUR

ex mod 11 A: (1, 4), B: (3, 7), C: (5, 1), D: (7, 2)

$\frac{7-4}{3-1} = \frac{3}{2}$

$2 \cdot 6 \equiv 1 \pmod{11}$

$6 \cdot 3 \equiv 7 \pmod{11}$

$7x + b \pmod{11}$

$b = 8$

$7x + 8 \pmod{11}$

$\frac{3}{4}$

$2 = a_0 + 7a_1$

$1 = a_0 + 5a_1$

$a_1 = \frac{1}{2}$ $10x + b \pmod{11}$

$\frac{3}{2} x$ $a_2 = -\frac{3}{2}$

$4 = a_0 + a_1$

$7 = a_0 + 3a_1$

$-\frac{4}{6}$ 4

$6 \cdot 2$ -12

$6 \cdot 9 \equiv 10 \pmod{11}$

$5 \cdot 9 \equiv 10 \pmod{11}$

$a_1 = \frac{3}{2}$

$a_0 = \frac{5}{2}$

$7 = a_0 + 3a_1$

$2 = a_0 + 7a_1$

$-\frac{5}{4}$

$4 \cdot 14 \equiv 1 \pmod{11}$

$4 \cdot 5 \equiv$

$6 \cdot 2$

$\frac{43}{4}$

$a_1 = -3$

$a_0 = 16$

$1 = a_0 + 5a_1$

$f(x) = \frac{3}{2} + \frac{5}{2} x$

$f(x) = 16 - 3x$

$f(x) = 43/4 - 5/4x$

Quadratic residues mod 5:

$1^2 \equiv \boxed{1} \pmod 5$ $4^2 \equiv \boxed{1} \pmod 5$

$2^2 \equiv \boxed{4} \pmod 5$

$3^2 \equiv \boxed{4} \pmod 5$

$\boxed{1, 4}$

Primitive roots:

order of a mod n is least $m \in \mathbb{N}$: $a^m \equiv 1 \pmod n$ $\quad \text{ord}_n a = m$

$a^k \equiv 1 \pmod n \iff \text{ord}_n a \mid k$

ex $n = 13$ $\quad \varphi(13) = 12$ $\quad 1, 2, 3, 4, 6, 12$

$2^1 = 2$ $\quad 2^2 = 4$ $\quad 2^3 = 8$ $\quad 2^4 = 16 \equiv 3$ $\quad 2^6 = 12 \equiv -1 \iff \text{ord}_{13} 2 = 12$

2 is primitive root

ex $n = 8$ $\quad \varphi(8) = 8 \cdot (1 - \frac{1}{2}) = 4$ $\quad 1, 2, 4$

possible primitive roots: $1, 3, 5, 7 \rightarrow \text{ord} = 2$

$3^2 = 9 \equiv 1$ $\quad 5^2 = 25 \equiv 1$ $\quad 7^2 = 49 \equiv 1$ $\quad$ no primitive roots mod 8

$n = 22$ $\quad \varphi(22) = 22 \cdot (1 - \frac{1}{11})(1 - \frac{1}{2}) = 10$

$\{1, 3, 5, 7, 9, 13, 15, 17, 19, 21\}$

must be divisors of $\varphi(22) = 10 = \{1, 2, 5, 10\}$

$3^1 = 3$ $\quad 3^2 = 9$ $\quad 3^5 = 1$ $\quad \text{ord}_3 = 5$ $\quad \text{ord}_7 = 10$, 7 is primitive root mod 22

Quadratic reciprocity:

$a \in \mathbb{Z}_p^*$ is a quadratic residue mod p if $x^2 \equiv_p a$ has a solution

$\left(\frac{a}{p}\right) = \begin{cases} +1 & a \text{ is quadratic residue} \\ -1 & \text{if } a \text{ isn't} \\ 0 & \text{if } \gcd(a, p) \neq 1 \end{cases}$

$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases}$ $\quad \left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 7 \pmod 8 \\ -1 & \text{if } p \equiv 3, 5 \pmod 8 \end{cases}$ $\quad \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} 1 & p \text{ or } q \equiv 1 \pmod 4 \\ -1 & p \equiv q \equiv 3 \pmod 4 \end{cases}$

ex $\left(\frac{31}{103}\right) = (-1)\left(\frac{103}{31}\right) = -\left(\frac{10}{31}\right) = -\left(\frac{2}{31}\right)\left(\frac{5}{31}\right) = (-1)\left(\frac{5}{31}\right) = (-1)\left(\frac{31}{5}\right) = -\frac{1}{5} = -1$

$\left(\frac{139}{433}\right) = (1)\left(\frac{433}{139}\right) = \left(\frac{16}{139}\right) = \left(\frac{4^2}{139}\right) = 1$

$\left(\frac{523}{1103}\right) = (-1)\left(\frac{1103}{523}\right) = -\left(\frac{57}{523}\right) = -\left(\frac{523}{57}\right) = -\left(\frac{10}{57}\right) = -\left(\frac{2}{57}\right)\left(\frac{5}{57}\right) = -\left(\frac{5}{57}\right) = \left(-\frac{57}{5}\right) = -\frac{2}{5}$

$= -(-1) = 1$

$\left(\frac{3}{97}\right) = (1)\left(\frac{97}{3}\right) = \left(\frac{1}{3}\right) = -\left(-\frac{1}{3}\right) = (-1)(-1) = 1$

$\left(\frac{3}{389}\right) = (-1)\left(\frac{389}{3}\right) = (+1)\left(\frac{2}{3}\right) = (-1)$

$\left(\frac{880}{863}\right) = \left(\frac{17}{863}\right) = \frac{863}{17} = \frac{13}{17} = \frac{17}{13} = \frac{4}{13} = \frac{2}{13} \cdot \frac{2}{13} = (-1)(-1) = 1$

Alice & Bob

↓

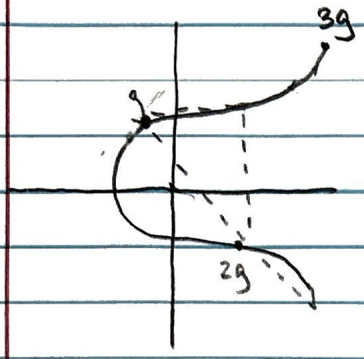
private: $1 \leq d \leq n-1$

public: $d \times G = (x_G, y_G)$

$P = d \times G$ $Q = e \times G$

$R = d \times Q = e \times P$

Elliptic Curve Cryptography:



~~Share a bit array number~~

$y^2 = x^3 + ax + b$

$\{p, a, b, G, n, h\}$

p - field defined over h - cofactor

a, b - values defining curve

G - fixed point we'll start at

n - prime order of G

Quizzes:

* $G = \mathbb{Z}_7^*$ is cyclic

$3^1 \equiv 3$ $3^2 \equiv 2$ $3^3 \equiv 6$ $3^4 \equiv 4$ $3^5 \equiv 5$ $3^6 \equiv 1$ so cyclic

$2^1 \equiv 2$ $2^2 \equiv 4$ $2^3 \equiv 1$ $2^4 \equiv 2$ $2^5 \equiv 4$ $2^6 \equiv 1$ $1^1 \equiv 1^2 \equiv \ldots \equiv 1^6 \equiv 1$

$\{1\}$ & $\{1, 2, 4\}$ are proper subgroups

* $2^{2^n} + 1$ last digit is 7 for $n \in \mathbb{N} \geq 2$

base case: $2^2 + 1 = 17$

$2^{2^{k+1}} + 1 = 2^{2^k} \cdot 2^{2^k}$ by I.H we know 2^{2^k} ends in 6 . _ 6 . _ 6

$= \_\ 6 \quad + 1 = \ldots 7$

* Remainder when 16! is divided by 19

*Wilson's theorem $\Rightarrow (p-1)! \equiv 1 \pmod p \Rightarrow 18! \equiv -1 \pmod{19}$

$\Rightarrow 18! \cdot 18^{-1} \equiv -1 \cdot 18^{-1} \equiv 18! \cdot 18^{-1} \cdot 17^{-1} \equiv -1 \cdot 18^{-1} \cdot 17^{-1} \pmod{19}$

$17^{-1} \equiv 9 \pmod{19}$ $18^{-1} \equiv -1$

$\Rightarrow 16! \equiv -1 \cdot -1 \cdot 9 \equiv 9 \pmod{19}$

HW Problems

- multiplicative inverse of $11 \pmod{17}$

$17 = 1 * 11 + 6$
$11 = 1 * 6 + 5$
$6 = 1 * 5 + 1$

$6 = 17 - 1 * 11$
$5 = 11 - (1 * (17 - 1 * 11))$
$1 = 17 - 1 * 11 - (11 - (1 * (17 - 1 * 11)))$
$= -3 * 11 + 2 * 17$

$-3 \pmod{17} \equiv 14 \pmod{17}$

- multiplicative inverse of $17 \pmod{11}$

$17 \pmod{11} \equiv 6 \pmod{11}$

$11 = 1 * 6 + 5$
$6 = 1 * 5 + 1$

$5 = 11 - 1 * 6$
$1 = 6 - (1 * (11 - 1 * 6))$
$= 6 * 2 - 1 * 11$
$17^{-1} \pmod{11} \equiv 2 \pmod{11}$

- 17 monkeys, 11 piles equal size, >7 per pile, remainder of 6, 17 groups

$17x \equiv 6 \pmod{11}$ $\quad \gcd(17, 11) = 1 \mid 6$

$17 = \boxed{1} * 11 + 6$

↙

solution 1, separated by 11, so 12

$6^{2000} / 11$

$(6^2)^{1000} \pmod{11} \equiv 3^{1000} \pmod{11} \equiv 4^{250} \pmod{11}$

$\equiv 5^{125} \pmod{11} \equiv (5^5)^{25} \pmod{11} \equiv (1)^{25} \pmod{11} \equiv 1 \pmod{11}$

* use fermat's little theorem

$1^{p-1} + 2^{p-1} + \ldots + (p-1)^{p-1}$

$1 + 1 + \ldots + 1$

$1 + 2 + \ldots + (p-1)$ $\qquad \frac{(p-1)p}{2} = \frac{p^2-p}{2}$

$\frac{p^2}{2} - \frac{p}{2}$ $\qquad$ p is even so $\frac{p}{2} \in \mathbb{Z}$, $\frac{p^2}{2} \in \mathbb{Z}$,

so $\frac{p^2}{2} - \frac{p}{2} \equiv 0 \pmod{p}$

$1^2 \not\equiv 0 \pmod{2}$ or $\frac{3^2}{2} - \frac{3}{2} = 3 \not\equiv 0 \pmod{2}$

Exam problem

- prove that for any integers x and y such that $x > y$ and $n = x^4 - y^4$ we have that $\varphi(n) < n-1$, where φ is the Euler phi function

$n = x^4 - y^4 = (x^2+y^2)(x^2-y^2) = (x^2+y^2)(x+y)(x-y)$

$x^2+y^2, x^2-y^2 \in \mathbb{Z}^+$, thus n is composite and isn't prime.

Suppose $j, k, i \in \mathbb{Z}$ where $j = x^2+y^2$, $k = x+y$, $i = x-y \mid n$.

If p is prime then $\varphi(p) = p-1$. Therefore, because n has at least 3 factors $\varphi(n) \leq n-4 < n-1$, proving $\varphi(n) < n-1$ given the conditions are met.

Pollard Factoring Method

Factor 1403

$2^{2!} \equiv 4 \pmod{1403}$ $\quad 2^{2!}-1 \equiv 3$ $\quad \gcd(3,1403)=1$

$2^{3!} \equiv 64$ $\quad 2^{3!}-1 \equiv 63$ $\quad \gcd(63,1403)=1$

$2^{4!} \equiv 142$ $\quad 2^{4!}-1 \equiv 141$ $\quad \gcd(141,1403)=1$

$2^{5!} \equiv 794$ $\quad 2^{5!}-1 \equiv 793$ $\quad \gcd(793,1403)=61$

$61 * 23 = 1403$

Factor 2993

$2^{2!} \equiv 4 \pmod{2993}$ $\quad \gcd(3,2993)=1$

$2^{3!} \equiv 64$ $\quad \gcd(63,2993)=1$

$2^{4!} \equiv 1451$ $\quad \gcd(1450,2993)=1$

$2^{5!} \equiv 1395$ $\quad \gcd(1394,2993)=41$

$41 * 73$

Test Q $\quad p > 5$ and prime

$\Rightarrow 7, 11, 13, \ldots$

$$2^{p-2} + 3^{p-2} + 6^{p-2} \equiv a \pmod{p}$$

$$\Rightarrow 2^{-1}2^{p-1} + 3^{-1}3^{p-2} + 6^{-1}6^{p-1} \equiv a \pmod{p}$$

$$\Rightarrow 6(2^{-1}2^{p-1} + 3^{-1}3^{p-1} + 6^{-1}6^{p-1}) \equiv 6a \pmod{p}$$

b/c p is prime, $\gcd(2,p)=1$, $\gcd(3,p)=1$, $\gcd(6,p)=1$, thus we can use Fermat's Little Theorem

$$\Rightarrow 3(1) + 2(1) - 1 \equiv 6a \pmod{p}$$

$$6 \equiv 6a \pmod{p}$$

$$1 \equiv a \pmod{p}$$

$$\Rightarrow 2^{p-2} + 3^{p-2} + 6^{p-2} \equiv 1 \pmod{p}$$

Euler function

$\varphi(n) = \#\{1 \le m \le n \mid \gcd(m,n) = 1\}$

If $\gcd(a,n) = 1$ then $a^{\varphi(n)} \equiv 1 \pmod{n}$

$5^{12} \equiv \_ \pmod{36}$ $\quad \varphi(36) = 36\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) = 12$

$3^{44} \equiv (3^4)^{11} \pmod{10}$ $\quad \varphi(10) = 10\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right) = 4$

$\equiv (1)^{11} \pmod{10} \equiv 1 \pmod{10}$

$7^{30} \equiv (7^8)^{3} 7^6 \pmod{15}$ $\quad \varphi(15) = 15\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 8$

$\equiv (1)^4 7^6 \pmod{15}$ $\quad 7^2 \equiv 4 \pmod{15}$

$\equiv (7^2)^3 \equiv \_ \pmod{15}$

$64 \pmod{15} \equiv 4 \pmod{15}$

$23^{130} \equiv (23^{20})^{6} \cdot 23^{10} \pmod{25}$ $\quad \varphi(25) = 25\left(1-\frac{1}{5}\right) = 20$

$\equiv (1)^6 \cdot 23^{10} \pmod{25} \equiv 23^{10} \pmod{25} \equiv -2^{10} \pmod{25}$

$\equiv (4)^5 \pmod{25}$ $\quad \equiv (2^5)^2 \equiv (-7)^2 \pmod{25}$

$\equiv 49 \pmod{25} \equiv -1 \pmod{25} = 24 \pmod{25}$

* If $\gcd(m,n) = 1$ then $\varphi(mn) = \varphi(m) \cdot \varphi(n)$

ex: $15 = 3 \cdot 5$

(1)	(2)	3
(4)	5	6
(7)	(8)	9
10	(11)	12
(13)	(14)	15

* $\varphi(3)$ columns with #s relatively prime to 3
* In each of these columns there are $\varphi(5)$ #s relatively prime to 5.

$\varphi(15) = \varphi(3) \cdot \varphi(5) = 2 \cdot 4 = 8$

$\varphi(p^r) = p^r - p^{r-1}$ $\qquad \varphi(n) = n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right)$

* Let a, b and m be integers such that $m > 0$ and $(a, m) = d$. If $d \nmid b$, then $ax \equiv b \pmod{m}$ has no solutions. If $d \mid b$, then $ax \equiv b \pmod{m}$ has exactly d incongruent solutions mod m.

Ex: $10x \equiv 3 \pmod{15}$

$\gcd(10, 15) = 5 \nmid 3$ * can't solve

Ex: $143x \equiv 44 \pmod{231}$

$\gcd(143, 231) = 11 \mid 44$ solutions $\frac{231}{11} = 21$

$231 = 1 \cdot 143 + 88$
$143 = 1 \cdot 88 + 55$
$88 = 1 \cdot 55 + 33$
$55 = 1 \cdot 33 + 22$
$33 = 1 \cdot 22 + (11)$
$22 = 2 \cdot 11 + 0$

$143x_0 + 231y_0 = 11$
$88 = 231 - 1 \cdot 143$
$55 = 143 - 1 \cdot 88$
$33 = 88 - 1 \cdot 55$
$22 = 55 - 1 \cdot 33$
$11 = 33 - 1 \cdot 22$

$55 = 143 - 1 \cdot (231 - 1 \cdot 143)$
$55 = 143 \cdot 2 - 231$
$33 = (231 - 1 \cdot 143) - 1 \cdot (143 \cdot 2 - 231)$
$33 = 2 \cdot 231 - 3 \cdot 143$

$22 = 143 \cdot 2 - 231 - 1 \cdot (2 \cdot 231 - 3 \cdot 143)$
$22 = 143 \cdot 5 - 3 \cdot 231$
$11 = 2 \cdot 231 - 3 \cdot 143 - 1 \cdot (143 \cdot 5 - 3 \cdot 231)$
$11 = 5 \cdot 231 - 8 \cdot 143$
$44 = 20 \cdot 231 - 32 \cdot 143$

$-32 \equiv 199 \pmod{231}$

$x = 199, 220, \ldots$
11 times

Chinese Remainder Theorem

$x \equiv 1 \pmod{3}$
$x \equiv 2 \pmod{5}$
$x \equiv 3 \pmod{7}$

$m = 3 \cdot 5 \cdot 7 = 105$
$m_1 = 105/3 = 35$
$m_2 = 105/5 = 21$
$m_3 = 105/7 = 15$

$35y_1 \equiv 1 \pmod{3}$
$y_1 \equiv 2 \pmod{3}$

$21y_2 \equiv 1 \pmod{5}$
$y_2 \equiv 1 \pmod{5}$

$15y_3 \equiv 1 \pmod{7}$
$y_3 \equiv 1 \pmod{7}$

$x \equiv 1 \cdot 35 \cdot 2 + 2 \cdot 21 \cdot 1 + 3 \cdot 15 \cdot 1 \equiv 157 \equiv 52 \pmod{105}$

$x \equiv 2 \pmod 3$
$x \equiv 3 \pmod 7$
$x \equiv 9 \pmod{10}$

$N = 210$
$N_1 = 70 \quad N_2 = 30 \quad N_3 = 21$

$x_1 \equiv N_1^{-1} \pmod{n_1} \equiv (70)^{-1} \pmod 3 \equiv 1^{-1} \pmod 3 \equiv 1 \pmod 3$
$x_2 \equiv (30)^{-1} \pmod 7 \equiv 2^{-1} \pmod 7 \equiv 4 \pmod 7$
$x_3 \equiv (21)^{-1} \pmod{10} \equiv 1^{-1} \pmod{10} \equiv 1 \pmod{10}$

$x = 2 \cdot 70 \cdot 1 + 3 \cdot 30 \cdot 4 + 9 \cdot 21 \cdot 1 = 689 \equiv 59 \pmod{210}$

Wilson's Theorem

$(p-1)! \equiv -1 \pmod p$: p is prime $\Leftrightarrow (p-2)! \equiv 1 \pmod p$

* Let p be an odd prime. Then $x^2 \equiv -1 \pmod p$ has a solution $\Leftrightarrow p \equiv 1 \pmod 4$

Corollary: There are infinitely many primes $\equiv 1 \pmod 4$

Pf BWOC sps $p_1, \dots, p_n$ are all of the primes $\equiv 1 \pmod 4$.
$N = 4(p_1, \dots, p_n)^2 + 1 \equiv 1 \pmod 4$
Sps $p \mid n \Rightarrow N \equiv 0 \pmod p$
$(2p_1, \dots, p_n)^2 \equiv -1 \pmod p$
$\Rightarrow p \equiv 1 \pmod 4 \Rightarrow p = p_i \quad 1 \le i \le n$
$p_i \mid N, \ p_i \mid 4(p_1, \dots, p_n)^2, \Rightarrow p_i \mid 1 \Rightarrow p_i = 1$ * contradiction

Wilson's Theorem

$(p-1)! \equiv -1 \pmod p$ where p is prime

* if you want to know if a number n is prime, then check $(n-1)! \pmod n$ and if it's -1 it's prime, if not -1, not prime

Fermat's little Theorem

If p is prime and $a \in \mathbb{Z}$ with $p \nmid a$, then $a^{p-1} \equiv 1 \pmod p$

Infinitely many primes?

- Euclid's proof ($Q_n = P_1 P_2 P_3 \ldots P_n + 1$)

If n is composite, n has a prime factor not exceeding $\sqrt{n}$

$1 < a \leq b < n$ $\quad a \leq \sqrt{n}$, otherwise $b \geq a > \sqrt{n}$ $\quad ab > \sqrt{n} \cdot \sqrt{n}$

Arithmetic progression

constant difference between successive numbers (3, 6, 9, 12)

Dirichlet's theorem

$a, a+d, a+2d, \ldots$ contains infinite primes (a & d are coprime)

Prime number theorem & Legendre's discovery

$$\pi(x) = \frac{x}{\ln(x)} \approx \frac{x}{\ln(x) - 1.08366}$$

Bertrand's conjecture

there's always at least 1 prime between n and $2n-2$ ($n > 1$)

Goldbach's conjecture

every integer > 2 can be expressed as sum of prime numbers

Legendre's conjecture

at least 1 prime between consecutive two squares

* riemann zeta function & hypothesis

Triangle numbers

$$T_n = \frac{n(n+1)}{2}$$

Infinitely many twin primes

$$P = (p_1 \cdot p_2 \cdot p_3 \ldots p_k)^2 - 1$$

IF P is prime then $(P-1), (P+1)$ are ime

Gaussian primes

same as * primes but for complex numbers

$z = a + bi$ is prime if:

1) a & b are integers
2) z is not $1, -1, i, -i$
3) if z can be expressed as the product of two non-units Gaussian integers, then those factors must be associates of z (differing only by units)

Greatest common divisor

- if $a, b \in \mathbb{Z}$ $(a, b \neq 0)$, $\gcd(a,b) = d$ $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$
- Any rational number a/b can be expressed in lowest terms (simplified) where $(a, b) = 1$
- if $a|b$ & $b|c$ then $a|c$

Euclidean Algorithm

$(252, 198)$

$252 = 1 \cdot 198 + 54$
$198 = 3 \cdot 54 + 36$
$54 = 1 \cdot 36 + \boxed{18}$ * gcd is last non-zero remainder
$36 = 2 \cdot 18$

Fundamental theorem of arithmetic

every positive integer > 1 can be expressed as a unique product of prime numbers (*order not included)

Congruences

$a \equiv b \pmod m$ means $m | (a-b)$

$a \equiv a \pmod m$, $a \equiv b \pmod m = b \equiv a \pmod n$

Linear congruences

$ax \equiv b \pmod m \equiv ax - my = b$

TEAM NAMES: Quinten Lang, Andrew Ebert, Samuel Tiktin, Owais Gavni

Applied Number Theory, Professor E. Gethner, Quiz 5, 2024

Instructions: Be neat, write complete sentences, and show all of your work. The way you communicate the solution to your answer is as important as the answer itself. This quiz is worth 100 points.

1. **(20 points)**

   (a) (15 points) Let $x^3 + ax^2 + bx + c$ be a cubic polynomial with roots r_1, r_2, and r_3. Prove that $r_1 + r_2 + r_3 = -a$. Show all of your work and don't leave out any details.

Assume we're given a polynomial $x^3 + ax^2 + bx + c$ with roots r_1, r_2, r_3; that is $x^3 + ax^2 + bx + c = (x - r_1)(x - r_2)(x - r_3) \Rightarrow$ $x^3 - (r_1 + r_2 + r_3)x^2 + (r_1r_2 + r_2r_3 + r_1r_3)x - r_1r_2r_3 \Rightarrow r_1 + r_2 + r_3 = -a$ as desired. Therefore cubic polynomial $x^3 + ax^2 + bx + c$ with roots r_1, r_2, r_3 gives us $r_1 + r_2 + r_3 = -a$

$\Rightarrow -(r_1 + r_2 + r_3) = a \Rightarrow$

   (b) (5 points) Write $x = x_1 - \frac{a}{3}$. Prove that $x^3 + ax^2 + bx + c = {x_1}^3 + b'x_1 + c'$ where $b' = b - (\frac{1}{3})a^2$, and $c' = c - (\frac{1}{3})ab + (\frac{2}{27})a^3$. Show all of your work and don't leave out any details. *Remark.* This problem shows that a simple change of variables converts an arbitrary cubic polynomial into one whose x^2 term has coefficient 0.

SW $x^3 + ax^2 + bx + c \Rightarrow \left(x_1 - \frac{a}{3}\right)^3 + a\left(x_1 - \frac{a}{3}\right)^2 + b\left(x_1 - \frac{a}{3}\right) + c$

$\left(x_1 - \frac{a}{3}\right)^2 = x_1^2 - 2x_1\frac{a}{3} + \frac{a^2}{9}$ $\Downarrow$ $\left(x_1^3 - 3x_1^2\frac{a}{3} + 3x_1\frac{a^2}{9} - \frac{a^3}{27}\right) + a\left(x_1^2 - 2x_1\frac{a}{3} + \frac{a^2}{9}\right)$

$\left(x_1 - \frac{a}{3}\right)^3 = x_1^3 - 2x_1^2\frac{a}{3} + \frac{a^2}{9}x_1$ $+ b\left(x_1 - \frac{a}{3}\right) + c$

$- x_1^2\frac{a}{3} + 2x_1\frac{a^2}{9} - \frac{a^3}{27}$ $\Downarrow$

$x_1^3 - x_1^2a + x_1\frac{a^2}{3} - \frac{a^3}{27} + x_1^2a - 2x_1\frac{a^2}{3} + \frac{a^3}{9}$

$+ x_1b - \frac{ab}{3} + c$

$x_1^3 - x_1\left(\frac{a^2}{3} + b\right) + \frac{2a^3}{27} - \frac{ab}{3} + c \Rightarrow x_1^3 + b'(x_1) + c'$ where $b' = b - \frac{a^2}{3}$ $c' = c - \frac{ab}{3} + \frac{2a^3}{27}$

Pf We want to prove $x^3+ax^2+bx+c = x_1^3+b'x_1+c'$ where $x = x_1 - \frac{a}{3}$.

So we begin under that assumption, plugging in $x_1-\frac{a}{3}$ for x;

$x^3+ax^2+bx+c \Rightarrow \left(x_1-\frac{a}{3}\right)^3 + a\left(x_1-\frac{a}{3}\right)^2 + b\left(x_1-\frac{a}{3}\right)+c$

$\Rightarrow \left(x_1^3 - 3x_1^2\frac{a}{3} + 3x_1\frac{a^2}{9} - \frac{a^3}{27}\right) + a\left(x_1^2 - 2x_1\frac{a}{3} + \frac{a^2}{9}\right) + b\left(x_1-\frac{a}{3}\right)+c$

$\Rightarrow x_1^3 - x_1^2a + x_1\frac{a^2}{3} - \frac{a^3}{27} + x_1^2a - 2x_1\frac{a^2}{3} + \frac{a^2}{9} + x_1b - \frac{ab}{3} + c$

$\Rightarrow x_1^3 + x_1\left(b-\frac{a^2}{3}\right) + \left(\frac{2a^3}{27} - \frac{ab}{3} + c\right)$. From here we use the values given for b' and c'. Plug in b' where $b' = b - \frac{a^2}{3}$ and plug in $c' = c - \frac{ab}{3} + \frac{2a^3}{27}$; this gives $x_1^3 + x_1(b') + c'$. Thus, we have proved $x^3+ax^2+bx+c = x_1^3 + b'x_1 + c'$, where $x = x_1 - \frac{a}{3}$, $b' = b - \frac{a^2}{3}$, $c' = c - \frac{ab}{3} + \frac{2a^3}{27}$, as desired.

TEAM NAMES: Quinten Lang, Andrew Ebert, Samuel Tiktin, Owais Garni

Number Theory, Professor E. Gethner, Quiz 3, 2024

Instructions: Be neat, write complete sentences, and show all of your work. The way you communicate the solution to your answer is as important as the answer itself. This quiz is worth 100 points..

1. (40 points) What is the remainder when 16! is divided by 19? *To receive credit for this problem you must write complete sentences, include all details, be clear and precise in your reasoning. Be sure to cite by name any theorem that you use.*

SW

* wilsons theorem

$(p-1)! \equiv -1 \pmod p \implies 18! \equiv -1 \pmod{19}$

* p is prime

$\implies 18! \cdot 18^{-1} \equiv -1 \cdot 18^{-1} \pmod{19} \Rightarrow 18! \cdot 18^{-1} \cdot 17^{-1} \equiv -1 \cdot 18^{-1} \cdot 17^{-1} \pmod{19}$

$\implies 16! \equiv -1 \cdot 18^{-1} \cdot 17^{-1} \pmod{19}$

$17x \equiv 1 \bmod 19$

$x = 9$

$18x \equiv 1 \bmod 19$

$x = 18 = -1$

$19 = 1 * 17 + 2$

$17 = 8 * 2 + 1$

$2 = 19 - 17 * 1$

$1 = 17 - (8 * (19 - 17))$

~~$1 = 17 - (8 * 2)$~~

~~$1 = 17 - 8 * (19 - 2 * 17)$~~

$1 = 17 - (8 * 19) + 8 * 17$

$9 * 17 - 8 * 19 = 1$

$17^{-1} \equiv 9 \pmod{19}$

$\implies 16! \equiv -1 \cdot -1 \cdot 9 \pmod{19} \equiv 9 \pmod{19}$

or $16! \equiv 18 \cdot 18 \cdot 9 \pmod{19} = 9 \pmod{19}$

scratch paper

We can use Wilson's theorem to prove that the remainder when 16! is divided by 19 is 9. First, Wilson's theorem gives us the following:

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

Now we can substitute our $p=19$, which holds because our p is prime, according to Wilson's theorem.

$18! \equiv -1 \pmod{19} \Rightarrow 18! \cdot 18^{-1} \equiv -1 \cdot 18^{-1} \pmod{19} \Rightarrow 18! \cdot 18^{-1} \cdot 17^{-1} \equiv -1 \cdot 18^{-1} \cdot 17^{-1} \pmod{19}$

Now, we can use Euclid's extended algorithm to solve for 18^{-1} and $17^{-1} \pmod{19}$:

$19 = 1 * 17 + 2$
$17 = 8 * 2 + 1$
$\Rightarrow 1 = 17 - (8 * 19) + 8 * 17$
$1 = 9 * 17 - 8 * 19$
$17^{-1} \equiv 9$

$19 = 1 * 18 + 1$
$18^{-1} \equiv -1$

Thus, we can solve the equation from above.

$16! \equiv -1 \cdot -1 \cdot 9 \pmod{19} \Rightarrow 16! \equiv 9 \pmod{19}$

Therefore, the remainder when 16! is divided by 19 is 9.

TEAM NAMES: Quinten Lang, Andrew Ebert, Samuel Tiktin, Owais Garni

CSCI 4110/5110, Professor E. Gethner, Quiz 4, 2024

Instructions: Be neat, write complete sentences, and show all of your work. The way you communicate the solution to your answer is as important as the answer itself. This quiz is worth 100 points.

1. (40 points) As we learned in class, the set $\mathbb{Z}_m^*$ together with the operation *multiplication* is a group. Let $m = 9$ and observe that since $gcd(4, 9) = 1$ we know that $4 \in \mathbb{Z}_9^*$. Find the order of 4 in the group $\mathbb{Z}_9^*$. Write complete sentences, include all details, and be precise and clear in your reasoning.

Because $\gcd(4,9) = 1$, 4 is in $\mathbb{Z}_9^*$.

By Euler's Totient Function:

$\varphi(9) = 9 * (1 - 1/3) = 6$

$|1, 2, 4, 5, 7, 8| = 6$

and verifying $4 \in \mathbb{Z}_9^*$ Proving the above statement. Thus, we can now do powers of 4 (mod 9) until $4^k \equiv 1 \pmod 9$, $k \in \mathbb{N}$.

$4^1 \equiv 4 \pmod 9$

$4^2 \equiv 7 \pmod 9$

$4^3 \equiv 1 \pmod 9$ ✓

Thus the order of 4 in group $\mathbb{Z}_9^*$ is 3 because $4^3 \equiv 1 \pmod 9$.

TEAM NAMES: Quinten Lang, Andrew Ebert, Samuel Tiktin, Owais Garni

Number Theory, Professor E. Gethner, Quiz 2, 2024

Instructions: Be neat, write complete sentences, and show all of your work. The way you communicate the solution to your answer is as important as the answer itself. This quiz is worth 100 points.

1. (40 points) Prove that the last digit in the decimal expansion of $F_n = 2^{2^n} + 1$ is 7 if $n \geq 2$. Hint: use induction to show that the last decimal digit of 2^{2^n} is 6. *To receive credit for this problem, you must write complete sentences, be clear and precise in your reasoning, include all details of your work, and use the proper syntax and method for an induction proof.*

SW

base case: $2^{2^2} = 16$ $\quad 2^{2^2}+1 = 17$

2^{2^k} $\quad k=2$ $\quad 2^{2^k}+1$

step: $2^{2^{k+1}} = 2^{2^k} \cdot 2^{2^k}$ $\quad 2^{2^k}+1 = (2^{2^k} \cdot 2^{2^k}+1)$

$2^{2^2} = 16$

$2^{2^3} = 256$

$2^{2^4} = 65,536$

2^{2^k} - ends in 6

$n = 10p+6$

$(2^{2^k})^2 = n^2 = (10p+6)(10p+6)$

$= 100p^2 + 120p + 36$

$= 10(10p^2 + 12p) + 36$

$q \in \mathbb{Z}$

$10q$ - decimal expansion of 0

$10q + 36$ - decimal expansion of 6

$(2^{2^k})^2 + 1$ - decimal expansion of 7

$(10q + 36) + 1$

Hypothesis:

If $n \in \mathbb{Z}$ and $n \geq 2$, then the last digit in the decimal expansion of $F_n = 2^{2^n} + 1$ is 7.

scratch paper

Base case:

We want to prove $F_n = 2^{2^n} + 1$ has a last decimal digit of 7 under the assumption that $n \geq 2$ by first using induction to prove the last decimal digit of 2^{2^n} is 6. We'll first prove the statement is true for base case $n = 2$.

$$F_2 = 2^{2^2} = 16$$

Inductive step:

Assume the form holds for $k \in \mathbb{Z}$, $k \geq 2$ where k is arbitrary; that is, the last decimal digit of 2^{2^k} is 6. We need to show $2^{2^{(k+1)}}$ also has a last decimal digit of 6. This can be rewritten.

$$2^{2^{(k+1)}} = 2^{2^k} \cdot 2^{2^k}$$

Thus, we have the product of two arbitrary integers with last decimal digits of 6. Let $j = 10r + 6$ be the form of an integer with last decimal digit 6. That is 2^{2^k} can be written in the form $10p + 6$.

$$2^{2^k} \cdot 2^{2^k} \Rightarrow (10p+6)^2 = 100p^2 + 120p + 36 = 10(10p^2 + 12p) + 36$$

Therefore, the product of two integers with last decimal digit 6 also has a last decimal digit of 6 because it's of the form $10r + 6$ where $r = (10p^2 + 12p + 3)$.

Conclusion:

By mathematical induction, we have proven the last decimal digit of 2^{2^n} is 6; therefore, we have proven the last decimal digit of $2^{2^n} + 1$ is 7 because the statements are equivalent. That is, these hold under the assumption that $n \in \mathbb{Z}$ and $n \geq 2$.