Fermat's Theorem:

If the modulus P is prime, then $a^{P-1} \equiv 1$ (mod P) for all a $\neq$ 0 (mod P).

→ Whenever the modulus is prime, we can treat all the exponents (modulo P-1)

Another way to compute inverses a^{-1} (mod P)

- Euclid: find x and y gcd (a, P)
  ax + Py = 1
  $a^{-1} \equiv$ x (mod P)
- $Fermat\ a^{-1} \equiv a^{P-1}$ (mod P) *Compute using repeated squaring.

(all that matters in the exponent is the remainder (mod P-1), -1(mod P-1) ≡ P-1 (mod P-1))

Euler Theorem (Extended version of Fermat's Theorem to composite moduli)

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

*Note that if n = P is prime then φ(P) = P-1, $a^{\varphi(p)} \equiv a^{P-1} \equiv 1$(mod P)

Example:

n = 10, a= 3

Compute $3^{\varphi(10)} = 3^4$ (φ(10) = φ(2) x φ(5)

$\equiv 9^2$ = (2-1) (5-1)

$\equiv 81$ = 1 x 4 = 4)

$\equiv 1$ (mod 10)

None Example: $4^{\varphi(10)}$ mod (10)

Gcd(4,10) = 2 → $4^4 \equiv 16^2 \equiv 256 \equiv 6$ (mod 10) * Not equal to 1

*Euler's Theorem doesn't apply.

Basic principle for exponents to any modulus:

If we're working (mod n) we can treat all the exponents mod φ(n)

*This doesn't necessarily work if the base has factors in common with the exponent.

If gcd(n,m) = 1 then φ(n,m) = φ(n) x φ(m)   (φ(n) is a multiplicative function)

φ(36) ≠ φ(6) x φ(6)   * $\varphi(P^k) = P^{k-1}$ (P-1)

Example: $E(x) = x^7 \pmod{22}$

Find a decryption function, $D(y) = E^{-1}(x)$, so that D(E(x)) = x

Guess: $D(y) \equiv y^d \pmod{22}$

$(x^7)^d \equiv x \pmod{22}$

$7d \equiv 1 \pmod{\varphi(22)}$

$\varphi(22) = \varphi(2 \text{ x } 11) \rightarrow = \varphi(2) \text{ x } \varphi(11) \rightarrow = 1 \text{ x } 10 = 10$

Need $7d \equiv 1 \pmod{10}$

$d = 3$ $D(y) \equiv y^3 \pmod{22}$

$E(x) \equiv x^5 \pmod{22}$ *Doesn't have a decryption function because gcd(5, φ(22)) = 5 (not 1)

RSA invented by Rivest, Shamir, and Adlemann uses this idea to do public key cryptography.

(RSA Set Up)

Alice picks two big primes p and q, (both have 120 digits), She computes n = (p)(q)

She picks an encryption exponent e, gcd(e, (p-1)(q-1)) = 1

In practice e = 65537

Alice's Public Key is (n,e) *(She keeps p,q and d secret)

Alice tells everyone this key.

Anyone can use this key to send a message to Alice using: $E(x) \equiv x^e \pmod{n}$

To decrypt we need a decryption function $D(y) \equiv y^d \pmod{n}$

Alice computes $d \equiv e^{-1} \pmod{\varphi(n)}$ $\quad\quad \varphi(n) = (p-1)(q-1)$

$d \equiv e^{-1} (\text{mod} (p-1)(q-1))$ → Euclid's Algorithm

---

Why can't Eve find D(y)?

Eve has to factor n to compute φ(n)

No one knows a fast way to factor numbers this big