RSA Encryption

The two main requisite skills are

- finding multiplicative inverses mod(m)
  main tool is the Extended Euclidean Algorithm
- modular exponentiation
  We have seen/worked through an algorithm called **fast modular exponentiation**: very generally applicable

Modular exponentiation: some more tools

Theorem: [Fermat's Little Theorem] If p is prime, and $a \in \mathbb{Z}$, then $a^p \equiv a \pmod p$.

Ex.

$$2^{17} \bmod 17 = 2$$

$$100^{17} \bmod 17 \equiv 100 \pmod{17}$$

Ex.

$$55^{73} \bmod 7$$

$$55^{73} = 55^{70} \cdot 55^3 = (55^7)^{10} \cdot 55^3$$

$$\equiv (55)^{10} \cdot 55^3 \pmod 7$$

$$\equiv 55^7 \cdot 55^6 \equiv 55 \cdot 55^6 \equiv 55^7$$

$$\equiv 55 \pmod 7$$

$a^p \equiv a \pmod p$

cancel an a from both sides (valid since p prime, $p \nmid a$), to get

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

Some consequences that follow, if $p \nmid a$

- If p is prime, then $a^{p-1} \equiv 1 (\bmod\, p)$.
- If p is prime, then a^{p-2} is the multiplicative inverse of a in $\mathbb{Z}_p$.
- If $\gcd(a, p) = 1$ and $a^{p-1} \not\equiv 1 (\bmod\, p)$, then p is not prime.

Ex. Find mult. inverse of 11 in $\mathbb{Z}_{17}$.

Since 17 is prime and $17 \nmid 11$, we can conclude

$$11^{16} \equiv 1 \pmod{17}$$

Thus

$$11 \cdot 11^{15} \equiv 1 \pmod{17}$$

$\Rightarrow$ $11^{15} \bmod 17$ is mult. inv. of 11 in $\mathbb{Z}_{17}$.

$\pi(12) = |\{2,3,5,7,11\}| = 5$

$\varphi(12) = |\{1,\cancel{2},\cancel{3},\cancel{4},5,\cancel{6},7,\cancel{8},\cancel{9},\cancel{10},11,\cancel{12}\}| = 4$

Definition: As functions $\mathbb{Z}^+ \to \mathbb{Z}$, we define

- the **prime-counting function** π so that

$$\pi(n) = |\{p \text{ is prime} \mid p \leqslant n\}|.$$

  Due to the great interest in primes, this function was thoroughly investigated, with a major breakthrough being the **prime number theorem** (see p. 262).
- the **Euler totient function** φ so that

$$\varphi(n) = |\{a \in \mathbb{Z}^+ \mid a \leqslant n \text{ and } \gcd(a,n) = 1\}|.$$

Properties of φ:

- If p is prime, then $\varphi(p) = p - 1$
- If p is prime, then $\varphi(p^\alpha) = p^\alpha\left(1 - \frac{1}{p}\right)$
- If $\gcd(a,b) = 1$, then $\varphi(ab) = \varphi(a)\varphi(b)$.
- If the prime factorization of n is

$$n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_k^{\alpha_k},$$

  then

$$\varphi(n) =$$

$$\varphi(n) = \varphi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}) = \varphi(p_1^{\alpha_1}) \cdot \varphi(p_2^{\alpha_2}) \cdots \varphi(p_k^{\alpha_k})$$

$$= p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) \cdot p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right) \cdots p_k^{\alpha_k}\left(1 - \frac{1}{p_k}\right)$$

$$= \underbrace{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}}_{= n}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

$$= \boxed{n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)}$$

formula for $\varphi(n)$ requiring its prime factorization

Theorem: [Euler] If $\gcd(a,n) = 1$ then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Ex.] $37^{67} \bmod 120$

Know $\varphi(120) = 32$ (see next page)

$$37^{67} = 37^{64} \cdot 37^3 = (37^{32})^2 \cdot 37^3$$

$$\equiv 1 \cdot 37^3 \equiv 37^3 \pmod{120}$$

If p is prime

$$\varphi(p) = \left|\{1, 2, 3, \dots, \cancel{p}\}\right| = p-1$$

$$\varphi(p^2) = \left|\{1, 2, 3, 4, \dots, \cancel{p}, \right.$$

$$p+1, p+2, p+3, \dots, \cancel{2p},$$

$$2p+1, 2p+2, \dots, \cancel{3p},$$

$$\left.\underline{\cancel{p^2}}\}\right|$$

$$= p^2 - p$$

$$\varphi(p^3) = p^3 - p^2$$

generally

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha\left(1 - \frac{1}{p}\right)$$

Above, showed

$$\varphi(n) = \varphi(p_1^{\alpha_1} p_1^{\alpha_2} \cdots p_k^{\alpha_k}) = n\left(1 - \frac{1}{p_1}\right)\cdots\left(1 - \frac{1}{p_k}\right)$$

Ex.) $\varphi(120) = \varphi(2^3 \cdot 3 \cdot 5)$

$$= 120\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)$$

$$= 32.$$

Ex.) Find mult. inv. of 37 in $\mathbb{Z}_{120}$.

Since $\varphi(120) = 32$, and $\gcd(37, 120) = 1$, Euler's Thm says

$$37^{32} \equiv 1 \pmod{120}$$

That is,

$$37 \cdot 37^{31} \equiv 1 \pmod{120}$$

which means

$$37^{31} \bmod 120$$

is the multiplicative inverse of 37, in $\mathbb{Z}_{120}$.