Fermat's Little Theorem

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

for $1 \leq a < p$

e.g. $p = 127$

$$3^{126} \equiv 1 \pmod{127}$$

$$1 \equiv 3^{126} \equiv \left(3^{63}\right)^2 \equiv (-1)^2 \pmod{127}$$

$$-1 \equiv 126 \equiv 3^{63} \equiv 3 \cdot 3^{62} \equiv 126 \pmod{127}$$

$$42 \equiv 3^{62} \equiv \left(3^{31}\right)^2 \equiv (-13)^2 \pmod{127}$$

$$(-13) \equiv 114 \equiv 3^{31} \equiv 3 \cdot 3^{30} \equiv 38 \cdot 3 \pmod{127}$$

$$38 \equiv$$

$$800 \equiv -89 \equiv 3^{30} \equiv \left(3^{15}\right)^2 \equiv (66)^2 \pmod{127}$$

$$3^{15} \equiv 3 \cdot 3^{14} \equiv 66 \pmod{127}$$

$$22 \equiv 3^{14} \equiv \left(3^7\right)^2 \equiv 28^2 \pmod{127}$$

$$28 \equiv 3^7 \equiv 3 \cdot 3^6 \pmod{127}$$

$94 \equiv 3^6 \equiv (3^3)^2 = (27)^2 \pmod{127}$

$3^3 \equiv 27 \pmod{127}$

$$\begin{array}{r} 27 \\ 27 \\ \hline 189 \\ 54 \\ \hline 729 \end{array}$$

$$\begin{array}{r} 94 \\ 3 \\ \hline 282 \end{array}$$

$$\begin{array}{r} 127 \overline{)282} \\ 254 \\ \hline 28 \end{array}$$

$66 = 6 \cdot 11$

$$\begin{array}{r} 66 \end{array} \quad \begin{array}{r} 6 \cdot 11 \\ \hline 6 \cdot 6 \cdot 121 \\ \hline -6 \cdot 6 \cdot 6 = -8 \cdot 27 \end{array}$$

$$\begin{array}{r} -27 \\ \times \ 8 \\ \hline 216 \end{array} \quad \begin{array}{r} 100 \\ 8 \\ \hline 800 \end{array}$$

$$\begin{array}{r} 127 \overline{)216} \\ 127 \\ \hline -89 \end{array}$$

$$\begin{array}{r} 6 \\ 127 \overline{)800} \\ 762 \\ \hline \end{array}$$

$$\begin{array}{r} 38 \\ 3 \\ \hline 114 \equiv -13 \end{array}$$

$$\begin{array}{r} 127 \overline{)169} \\ 127 \\ \hline 42 \end{array}$$

Exercises:

1. Compute $\phi(50910363)$ knowing that

$$50910363 = 3^4 \times 7^2 \times 101 \times 127.$$

2. Use your answer from the previous question to compute

$$2^{28576807} \ mod \ 50910363.$$

3. Compute 3^{999} mod 143.

$143 = 11 \cdot 13$
$\phi(143) = 120$

$$\begin{aligned}\phi(50910363) &= (3^4-3^3)(7^2-7)(101-1)(127-1) \\ &= (81-27)(49-7)(100)(126) \\ &= 54 \cdot 42 \cdot 100 \cdot 126 \\ &= 28576800\end{aligned}$$

So $2^{28576800+7} = 2^{28576800} \cdot 2^7 \equiv$

$\equiv 1 \cdot 2^7 \pmod{50910363}$

$\equiv 128 \pmod{50910363}$

$3^{999} \equiv 3^{8 \cdot 120 + 39} \equiv 3^{39} \pmod{143}$

$$92 \equiv 3^{39} \equiv 3 \cdot 3^{38} \pmod{143}$$

$$126 \equiv 3^{38} \equiv \left(3^{19}\right)^2 \pmod{143}$$

$$81 \equiv \text{[illegible]}\ 3^{19} \equiv 3 \cdot 3^{18} \equiv 27 \cdot 3 \pmod{143}$$

$$27 \equiv 8464 \equiv 3^{18} \equiv \left(3^9\right)^2 \equiv (92)^2 \pmod{143}$$

$$92 \equiv 3^9 \equiv 3 \cdot 3^8 \equiv 3 \cdot 126 \pmod{143}$$

$$126 \equiv 3^8 \equiv \left(3^4\right)^2 \pmod{143}$$

$$3^4 \equiv 81 \pmod{143}$$

$$\begin{array}{r} 92 \\ 92 \\ \hline 184 \\ 828 \\ \hline 8464 \end{array} \qquad \begin{array}{r} 81^2 \\ 81 \\ \hline 81 \\ 648 \\ \hline 6561 \end{array} \qquad \begin{array}{r} 126 \\ 3 \\ \hline 378 \\ 286 \\ \hline 92 \end{array}$$

$m = 22$

Rel prime to $22 = 1, 3, 5, 7, 9, 13, 15, 17, 19, 21$

$\gcd(x, 22) = 1$

$\phi(22) = 10$

multiply this list by 7

Claim:

$7^{10} \equiv 1 \pmod{22}$

$7, 21, 13, 5, 19, 3, 17, \overset{119}{9}, \overset{133}{1}, 15$

$1 \equiv$

$\cancel{1} \cdot \cancel{3} \cdot \cancel{5} \cdot \cancel{7} \cdot \cancel{9} \cdot \cancel{13} \cdot \cancel{15} \cdot \cancel{17} \cdot \cancel{19} \cdot \cancel{21} \equiv$

$7 \cdot 21 \cdot 13 \cdot 5 \cdot 19 \cdot 3 \cdot 17 \cdot 9 \cdot 1 \cdot 15 \equiv$

$7 \cdot \cancel{1} \cdot 7 \cdot \cancel{1} \cdot 7 \cdot \cancel{3} \cdot 7 \cdot \cancel{5} \cdot 7 \cdot \cancel{9} \cdot 7 \cdot \cancel{13} \cdot 7 \cdot \cancel{15} \cdot 7 \cdot \cancel{17} \cdot 7 \cdot \cancel{19} \cdot 7 \cdot \cancel{21} \pmod{22}$

$7^{10} \equiv$

Quadratic Residues

Denote the set of quadratic residues by the symbol

$$QR[p] = \left\{ x^2 \bmod p \mid x \in \{1, 2, \dots p-1\} \right\}.$$

Example

1. $p = 11$

x	1	2	3	4	5	6	7	8	9	10
x^2	1	4	9	5	3	3	5	9	4	1

$$QR[11] = \{1, 4, 9, 5, 3\}.$$

2. $p = 13$

x	1	2	3	4	5	6	7	8	9	10	11	12
x^2	1	4	9	3	12	10	10	12	3	9	4	1

$$QR[13] = \{1, 4, 9, 3, 12, 10\}.$$

$X^2 \equiv 4 \pmod{13}$ has 2 solutions.

but $X^2 \equiv 5 \pmod{13}$ does not ~~a~~ have a solution

Theorem 3 *For any prime $p > 2$ and any integer a not equal to 0* $\pmod{p}$ *we have*

$$a^{(p-1)/2} = \begin{cases} 1 & \text{if } a \in QR[p] \\ -1 & \text{if } a \notin QR[p] \end{cases} \quad (\text{mod } p)$$

Proof.

If $a = x^2$ with $x \neq 0$ mod p then Fermat's theorem gives

$$a^{(p-1)/2} = x^{p-1} = 1 \pmod{p}$$

Thus the first part of our assertion holds true. To prove the second part, note that the equation

Will have at most p-1 solutions $\rightarrow$ $$x^{p-1} - 1 = 0 \pmod{p}$$

has exactly $p - 1$ solutions in $\{1, 2, \ldots, p - 1\}$ and for $p > 2$ we have the factorization

$$x^{p-1} - 1 = (x^{(p-1)/2} - 1)(x^{(p-1)/2} + 1). \quad (\text{mod } p)$$

All $(p - 1)/2$ elements of $QR[p]$ satisfy the first factor. Therefore the other $(p - 1)/2$ solutions must satisfy

$$x^{(p-1)/2} + 1 = 0.$$

Legendre Symbol

For a prime p

Don't ever use this notation if p is not a prime.

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \in QR[p] \\ -1 & \text{if } a \notin QR[p] \\ 0 & \text{if } gcd(a,p) > 1 \end{cases}$$

Then for a relatively prime to p, we have

$$\left(\frac{a}{p}\right) = a^{(p-1)/2} \mod p$$

if a & p are relatively prime.

Hence

$$ab^{\frac{p-1}{2}} = \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = a^{\frac{p-1}{2}} \cdot b^{\frac{p-1}{2}} \pmod{p}$$

Theorem 4 (Quadratic Reciprocity) *For any two primes p and q we have*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}$$

Primality Testing

The Jacobi symbol allows us to test for primality of n without carrying out its factorization.

if n is prime $= p$
$J(a,p) = \left(\frac{a}{p}\right)$

If n is prime then

$$J(a, n) = a^{(n-1)/2} \mod n$$

Thus if this identity fails to hold for any value of a in $[1, n-1]$ we can certainly conclude that n is not a prime!

Theorem 5 *If n is not a prime then for more than one half the integers in $\{1, \ldots, n-1\}$ one of the following two tests will fail*

$$J(a, n) = a^{(n-1)/2} \qquad \gcd(a, n) = 1$$

The RSA System

1. Choose p and q primes and let $m = pq$
2. Message space: $\{1, 2, \ldots, m-1\}$.
3. Key space: $\{e \mid 1 \leq e \leq \phi(m), gcd(e, \phi(m)) = 1\}$
4. Encrypting transformation

$$\boxed{C = E_e(M) = M^e \bmod m}$$

5. Decrypting transformation

$d = e^{-1} \pmod{\phi(m)}$

that is $d \cdot e \equiv 1 \pmod{\phi(m)}$

$$\boxed{M = D_d(C) = C^d \bmod m}$$

$\equiv$

where $ed \equiv 1 \bmod \phi(m)$

$(M^e)^d \equiv M^{ed} \equiv M^1 \pmod{m}$

$$\boxed{m,\ e \text{ public}} \qquad \boxed{p,\ q,\ d \text{ private}}$$

Pick $a_1, a_2, \ldots, a_{100}$ at random.

If n "passes" the test

$J(a_i, n) \equiv a^{n-1/2} \pmod{n}$

and $\gcd(a_i, n) = 1$ for all 100 integers then

$P(n \text{ is not prime}) = \frac{1}{2^{100}}$

$P(n \text{ is prime}) = 1 - \frac{1}{2^{100}}$