p prime

$$1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2$$

are all distinct mod p.

Because if $i^2 \equiv j^2 \pmod p$

then $i^2 - j^2$ is divisible by p

and $i^2 - j^2 = (i-j)(i+j)$

if i, j are both $\leq \frac{p-1}{2}$

then $i-j$ & $i+j$ are $< p$

$\Rightarrow$ $i-j = 0$ because p does not divide $i+j$ & so it must divide $i-j$ and since the only # $< p$ that p divides is 0.

Recall $i^2 \equiv (p-i)^2 \equiv p^2 - 2pi + i^2 \equiv$

So all the quadratic residues are

$$\left\{1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2\right\}$$

$$\begin{array}{r} 46 \\ 17 \overline{)787} \\ \underline{782} \\ 5 \end{array} \qquad \begin{array}{r} 46 \\ \underline{17} \\ 322 \\ \underline{46} \end{array}$$

$$J(17, 787) = J(787 \bmod 17, 17) \cdot \cancel{(-1)^{\frac{16 \cdot 786}{4}}}\ 1$$

$$= J(5, 17) \cdot 1$$

$$= J(17 \bmod 5, 5)(-1)^{\frac{4 \cdot 16}{4}}$$

$$= J(2, 5)$$

$$= J(2/2, 5)(-1)^{(25-1)/8}$$

$$= -J(1, 5) = -1$$

$$17^{393} \pmod{787} \equiv -1$$

$$5^{8} \equiv -1 \pmod{17}$$

$17^{395} = 17^{393} \cdot 17^2 \equiv -17^2 \pmod{787}$

Jacobi Symbol

there is no solution to $17 \equiv x^2 \pmod{787}$ $\Leftarrow$ $17^{\cancel{383}\,393} \pmod{787} = 17^{\frac{787-1}{2}} \pmod{787} = \left(\frac{17}{787}\right) = -1$

We start with the Legendre symbol

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

and for

$$n = p_1 p_2 \cdots p_k$$

we set

$$J(a,n) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_k}\right)$$

However, for n odd, we have

$$J(a,n) = \begin{cases} 1 & \text{if } a = 1 \\ J(a/2,n)(-1)^{(n^2-1)/8} & \text{if } a \text{ is even} \\ J(n \mod a, a)(-1)^{(n-1)(a-1)/4} & \text{if } a > 1 \text{ and odd} \end{cases}$$

Take a bunch of samples

$a_1, a_2, \ldots, a_k$

and test

$J(a_1, n)$ vs. $a_1^{\frac{n-1}{2}} \pmod{n}$

$J(a_2, n)$ vs. $a_2^{\frac{n-1}{2}} \pmod{n}$

$J(a_3, n)$ vs. $a_3^{\frac{n-1}{2}} \pmod{n}$

$\vdots$

$J(a_k, n)$ vs. $a_k^{\frac{n-1}{2}} \pmod{n}$

If $a_1, \ldots, a_k$ were chosen at random then because ~~the~~ $J(a_i, n) \not\equiv a_i^{\frac{n-1}{2}} \pmod{n}$ for half of the integers a, there is a $(1/2)^k$ chance that my a_i's were chosen so that $J(a_i, n) \equiv a^{\frac{n-1}{2}} \pmod{n}$ even though n is not prime.

Quadratic Sieve

$23^2 \equiv 16^2 \pmod{91}$

Example: $m = 91$

$(23+16) = 39 \quad 23-16 = 7$

a	19	1	23	18	2	24	16
a^2	88	1	74	51	4	30	74

$$\begin{aligned} 91 &= gcd(91, 23+16) \times gcd(91, 23-16) \\ &= gcd(91, 39) \times gcd(91, 7) \\ &= 13 \times 7 \end{aligned}$$

Exercises

1. An individual publishes an RSA modulus of $m = 350123$ and an encryption exponent $e = 37$. Find his decrypting exponent, given that one of the factors of m is 347.
2. Encrypt each letter of the word BANG individually using the RSA system with $m = 143$ and $e = 7$. In translating letters into numbers, send A to 10, B to 11, ..., Z to 35.
3. Using the same system described in the previous problem, find the decrypting exponent d and decode the message 132 (a single letter).
4. Factor $m = 773,771$ into the product of two primes given that $\phi(m) = 771,552$.

$$\underbrace{\phi(m)}_{=771552} = (p-1)(q-1) = \overbrace{pq}^{=773771} - p - q + 1$$

$$p + q = 773771 - 771552 + 1$$

$$p + q = 2220$$

$$p + \frac{773771}{p} = 2220$$

$$p = \frac{2220 \pm \sqrt{2220^2 - 4 \cdot 773771}}{2}$$

$$= 1787, 433$$

$$p^2 - 2220p + 773771 = 0$$

Diffie-Hellman Public Key Exchange

1. People $P_1, P_2, \ldots P_k$ agree on a modulus p in which they agree to do their calculations.

2. They also agree on a common base, a, which must be a primitive root of p

3. Each person P_i secretly selects a number, S_i, from 1 to $p-1$ and publicly announces the value $\beta_i = a^{S_i} \bmod p$.

Alice $a^{S_1} \longrightarrow E_1(X)$

Bob $a^{S_2} \longrightarrow E_2(X)$

they use common key $a^{S_1 S_2} = (a^{S_1})^{S_2} = (a^{S_2})^{S_1}$