T-79.5501
Cryptology

Lecture 8 (March 13, 2007):

- Euler’s criterion
- Jacobi symbol
- Solovay-Strassen test
- Miller-Rabin test
- Square roots modulo n (see also slides)

Square Roots $\mathbf{mod}\ n$

p, q primes, $p \neq q$, and $n = pq$, $0 < a < n$.

Congruence

$$x^2 \equiv a \pmod{n}$$

has solutions if and only if the system

$$\begin{cases} x^2 \equiv a \pmod{p} \\ x^2 \equiv a \pmod{q} \end{cases}$$

has solutions. If this system has a solution $x = b$, then it has four solutions that can be computed using the Chinese RT from:

$$\begin{cases} x \equiv \pm\, b \pmod{p} \\ x \equiv \pm\, b \pmod{q} \end{cases}$$

as the four possible combinations.

Square roots mod n

Example. Find the square roots of 1 modulo

$n = 402038951687077 = 20051107 \cdot 20050711$

To find the non-trivial square roots, we use CRT to compute x such that

$$x \equiv 1 \pmod{20051107}$$

$$x \equiv -1 \pmod{20050711}$$

We get $(20050711)^{-1} \bmod 20051107 = 8860969$

and $(20051107)^{-1} \bmod 20050711 = 19163917$. By CRT:

$$x = 1 \cdot 8860969 \cdot 20050711 + (-1) \cdot 19163917 \cdot 20051107$$

$$= 46701494489160.$$

The second nontrivial square root of 1 is $-x = 355337457197917$

Square roots modulo a prime power p^i

Exercise 5.24 Solution: Assume $\gcd(a,p) = 1$, $b^2 \equiv a \pmod{p^{i-1}}$, $x^2 \equiv a \pmod{p^i}$, and denote $x = b + k\,p^{i-1}$ where k is unknown.

We get

$x^2 \equiv (b + k\,p^{i-1})^2 \equiv b^2 + 2bk\,p^{i-1} + (kp^{i-1})^2 \equiv b^2 + 2bk\,p^{i-1} \pmod{p^i}$.

On the other hand, $x^2 \equiv a \pmod{p^i}$, and hence

$a - b^2 \equiv 2bk\,p^{i-1} \pmod{p^i}$. Dividing the equation by p^{i-1} we get

$$(a - b^2)/\,p^{i-1} \equiv 2bk \pmod{p}.$$

If $b \equiv 0 \pmod{p}$, then $a \equiv 0 \pmod{p}$, which contradicts $\gcd(a,p) = 1$.

As $b \neq 0 \pmod{p}$, we can compute $b^{-1} \pmod{p}$ and $2^{-1} \pmod{p}$

and get $k = b^{-1} \cdot 2^{-1}\,((a - b^2)/\,p^{i-1}) \pmod{p}$.

Example: $b = 6$, $a = 17$, $p = 19$, $i = 2$, gives $x = 215$

PRIMES

PRIMES: Given a positive integer n, answer the question: is n prime?

Clearly PRIMES $\in \mathcal{coNP}$, as compositeness of an integer can be checked in polynomial time given the factors.

Solovay-Strassen, Miller Rabin: PRIMES $\in \mathcal{coPP}$ (the negative answer can be given in polynomial time using a probabilistic polynomial-time algorithm)

Miller (1976): Generalised Riemann Hypothesis (if it holds) would imply that PRIMES $\in \mathcal{P}$

Agrawal, M., N. Kayal, and N. Saxena (2002) PRIMES $\in \mathcal{P}$. Available at http://www.cse.iitk.ac.in/primality.pdf.

The resulting algorithm still not practical.

Further Readings:

http://cr.yp.to/papers/aks.pdf