Number Theory

Fermat's Last Theorem:

$$X^a + Y^a = Z^a$$

We want integer solutions for fixed $a \geq 2$

$a=2 \Rightarrow 3; 4; 5$ (Pythagorean triplet)

$a \geq 3 \Rightarrow$ No solution

For us we'll consider $\mathbb{Z}_n : \{0, 1, 2, \dots, n-1\}$ for $n \in \mathbb{N}$, series of Integers mod n.

Also $(\mathbb{Z}_n, +)$ is a group. Properties of the group:

↳ sum in mod n

- CLOSURE: $\forall a, b \in \mathbb{Z}_n$, $a+b \in \mathbb{Z}_n$
- IDENTITY: $\exists 0 \in \mathbb{Z}_n$, s.t. $a+0=a$ $\forall a \in \mathbb{Z}_n$
- COMMUTATIVE: $a+b=b+a$ $\forall a, b \in \mathbb{Z}_n$
- INVERSE: $\forall a \in \mathbb{Z}_n$ $\exists -a \in \mathbb{Z}_n$ such that $a+(-a)=0$

Also notice that $(\mathbb{Z}_n, \cdot)$ is NOT a group, because

↳ product mod n

not every a is invertible.

greatest common divisor

THM If $\gcd(a,n) > 1$ then $a \in \mathbb{Z}_n$ is not invertible with respect to mult. mod n

Proof: By contraddiction, assume a is invertible

$\exists b \in \mathbb{Z}_n$ such that $a \cdot b = 1 \mod n$. Then
$a \cdot b = 1 + qn$ for some $q > 0$

But then $\gcd(a,n)$ divides $ab - qn = 1$
Which means $\gcd(a,n) = 1$. Contraddiction!

Define $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n : \gcd(a,n) = 1\}$

$$||\mathbb{Z}_n^*|| = \varphi(n)$$ Euler's Totient Function

If $n = p$ a prime, then $\mathbb{Z}_p^* = \{1, \dots, p-1\}$, and

$$\varphi(p) = p - 1$$

Operations in $\mathbb{Z}_n$:

- Additions and multiplications take $O(\log^2 \lambda)$ where $\lambda = |a|$
- Inverse (if $\exists$ exists) can also be computed efficiently by means of the EUCLIDIAN ALGORITHM

<u>LEMMA</u>: Let a, b s.t. $a \geq b > 0$. Then $\gcd(a,b) = \gcd(b, a \mod b)$

Proof: We have $a = qb + a \mod b$ for $q > 0$ where
$q = \lfloor a/b \rfloor$ is the quotient.

$\Rightarrow$ A common divisor for a and b is also a common divisor of $a - qb = a \mod b$

Also, a common divisor of b and $a \bmod b$ is a common divisor of $a = qb + a \bmod b$

$\Rightarrow \gcd(a,b) = \gcd(b, a \bmod b)$

<u>THM</u>: Given a, b we can compute $\gcd(a,b)$ in poly time.
Also, we can find u, v, such that
$\gcd(a,b) = au + bv$ Bézout's identity

Proof: Apply lemma:

$$a = bq_1 + r_1 \quad \text{with } 0 \le r_1 < b$$
$$r_1 = a \bmod b$$

and $\gcd(a,b) = \gcd(b, r_1)$. Similarly

$$b = r_1 q_2 + r_2 \quad \text{with } 0 \le r_2 < r_1$$

Keep going until $r_{t+1} = 0$, then

$$\gcd(a,b) = \gcd(b, r_1) = \dots = \gcd(r_t, \underbrace{r_{t+1}}_{=0}) = r_t$$

Complexity: We show t is bounded by a poly in $\lambda = |b|$.
We claim that $r_{i+2} \le r_i/2 \quad \forall\, 0 \le i \le t-2$
(every two steps in the algo, the remainder is halved)

Clearly $r_{i+1} < r_i$ so the series decreases.
Now if $r_{i+1} \le r_i/2$ we are done, because $r_{i+2} < r_{i+1} \le r_i/2$.
So, assume $r_{i+1} > r_i/2$. Then

$$\underset{i+2}{r_{i+1}} = r_i \bmod r_{i+1} = r_i - q_{i+2} \cdot r_{i+1}$$

$\leq r_1 - r_{i+1}$

$< r_i - r_i/2 = r_i/2$

$\Rightarrow$ # steps is $2(\lambda - 1)$

The values u, v can be formed by eversing the steps of the algorithm.

EXAMPLE: Take $a = 14$, $b = 10$. Then

$$14 = 1 \cdot 10 + 4;\ 10 = 2 \cdot 4 + 2;\ 4 = 2 \cdot 2 + 0$$

$$\Rightarrow \gcd(14, 10) = 2$$

Moreover, if we revert the steps:

$$2 = 10 - 2 \cdot 4 = 10 - 2(14 - 1 \cdot 10) = 3 \cdot 10 + (-2) \cdot 14$$

$$\Rightarrow u = -2,\ v = 3$$

So we can compute the inverse of a mod n if $\gcd(a, n) = 1$ we can find u, v s.t.

$$a \cdot u + n \cdot v = 1 \Rightarrow u = a^{-1} \bmod n$$

Next: exponentation mod n: $a^b \bmod n$.

This is also poly-time by SQUARE and MULTIPLY.

Write $b = b_0 b_1 \dots b_0$ in binary

$$a^b = a^{\sum_i b_i \cdot 2^i} = \prod_{i=0}^{t} a^{b_i \cdot 2^i} = \prod_{i : b_i = 1} a^{2^i}$$

$$= a^{b_0} \cdot (a^2)^{b_1} \cdot (a^4)^{b_2} \dots (a^{2^t})^{b_t} \bmod n$$

We now turn to study primes

THM (PNT): There are infinitely many primes, and

$$\pi(x) = \text{"number of primes} \le x\text{"} \geq \frac{x}{3\log_2 x} \approx \frac{x}{\log x}$$

Here, hence,

$$\Pr[x \text{ PRIME}: x \leftarrow\$ [2^\lambda - 1]] \geq$$

$$\geq \frac{2^{\lambda-1}/3\log(2^\lambda - 1)}{2^{\lambda-1}} \geq \frac{1}{3\lambda}$$

THM (Muller-Rabin) We can test in poly-time if $n=p$ is prime

Then we can efficiently sample LARGE PRIMES
Sample $x \leftarrow\$ [2^\lambda - 1]$ and test if prime
If not, sample again

$$\Pr[\text{No output after } t \text{ steps}] \leq \left(1 - \frac{1}{3\lambda}\right)^t$$

for $t = 3\lambda^2$, $\Pr \leq e^{-\lambda}$ NEPLERO CONSTANT

Given two λ-bit primes p and q we can compute $n = p \cdot q$ in poly(λ)-time.

CONJECTURE Integer multiplication of two λ-bit primes is a OWF.

Many attempts: QUADRATIC SIEVE, NUMBER FIELD SIEVE

Complexity is sub-esponential in λ.

DISCRETE LOG

<u>THM</u> (Lagrange). If $\mathbb{H}$ is a subgroup of $\mathbb{G}$, then

it is possible to divide the cardinalities

$$\# \mathbb{H} / \# \mathbb{G}$$

<u>COR</u> For all $a \in \mathbb{Z}_n^*$ it holds that:

$$a^{\varphi(n)} = 1 \bmod n$$ ($a^{p-1} = 1 \bmod p$ when $n = p$ a prime)

FERMAT'S LITTLE THEOREM

$$a^b = a^{b \bmod \varphi(n)} \bmod n$$

PROOF: $(\mathbb{Z}_n^*, \cdot)$ is a group with $\varphi(n)$ elements $\# \mathbb{Z}_n^*$.

By Lagrange, the SUBGROUP of the powers of a

$$a^0 = 1, a^2, a^3, \dots, a^{d-1}$$

has multiplicative order d divides $\varphi(n)$

i.e. $d \cdot k = \varphi(n)$ for some k

$$\Rightarrow a^{\varphi(n)} = (a^d)^k = 1 \bmod n$$

Also $a^b \equiv a^{q \cdot \varphi(n) + b \bmod \varphi(n)}$

$$\equiv \underbrace{a^{q \cdot \varphi(n)}}_{=1} \cdot a^{b \bmod \varphi(n)} \equiv a^{b \bmod \varphi(n)}$$

Notice that $(\mathbb{Z}_p^*, +, \cdot)$ is a FIELD, because

$$\forall a \in \mathbb{Z}_p^* \quad \gcd(a, p) = 1$$

But there's more! $(\mathbb{Z}_p^*, \cdot)$ is a CYCLIC GROUP.

$$\exists \overset{\text{generator}}{g} \in \mathbb{Z}_p^* \text{ s.t. } \mathbb{Z}_p^* = \{g^0, g^1, \dots, g^{p-2}\}$$

EXAMPLE: 3 is generator of $\mathbb{Z}_7^*$, but 2 is not.

Indeed, $\mathbb{Z}_7^* = \{3^0, 3^1, 3^2, 3^3, 3^4, 3^5\} = \{1, 3, 2, 6, 4, 5\}$

FACT We can sample efficiently a random generator of $\mathbb{Z}_p^*$ if we are given the factorization of $p-1$.

DIFFIE-HELLMAN KEY EXCHANGE (first PKE)

$(\mathbb{Z}_p^*, \cdot)$ with generator $g \in \mathbb{Z}_p^*$

Alice		Bob
$x \leftarrow \$ \{0, \dots, p-2\}$	$\xrightarrow{g^x}$	$y \leftarrow \$ \{0, \dots, p-2\}$
$k = (g^y)^x = g^{xy} \bmod p$	$\xleftarrow{g^y}$	$k = (g^x)^y = g^{xy} \bmod p$

What about security? Assume Eve is passive (only observes the communication).

Intuition: It should be hard to compute k

CONJECTURE: For λ-bit prime p the function

$f_{g,p}(x) = g^x \bmod p$ is a OWF

DISCRETE LOG ASSUMPTION

Many attempts: Only know SUB-EXP. algorithms.
Passive security of DH key exchange requires to assume DL problem is hard.
Is it enough? Maybe, we don't know.
There could be another way to compute $K = g^{xy}$ without computing x and y.

<u>CONJECTURE</u>. (computational DH assumption - CDH)

No PPT $\mathcal{A}$ can win the following

$$
\begin{array}{ccc}
\mathcal{A}(1^\lambda) & & \mathcal{C}(1^\lambda) \\
 & \xleftarrow{\quad p,\, g,\, g^x,\, g^y \quad} & x, y \leftarrow \$ \{0, \dots, p-2\} \\
 & \xrightarrow{\quad z \quad} & \mathcal{A} \text{ wins if} \\
 & & z = g^{xy} \bmod p
\end{array}
$$

CDH implies DL (as discussed above)

Does DL imply CDH? We don't know.
The only way we know how to break CDH is by breaking DL!