17-DEC-200

Mastemath Utrecht $14^{15} - 17^{00}$

- collect questionaires & list of participants (can also fill in q. online)

Topic: integer factorisation

Last week: motivation & Dixon's method (method of two squares)

Today: (p-1) - method and ECM

1) Pollard's (p-1) method

Let p be a prime. Then

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

for any a with $p \nmid a$.

Then $\gcd(a^{p-1} - 1, m)$ contains p if p divides m.

|| We will try to find p given m.

Pick $s = \mathrm{lcm}(\{1, 2, 3, 4, \ldots, B\})$ for some bound B.

Pick a random $1 < a < m$ and compute

$$\gcd(a^s - 1, m)$$

If $(p-1) \mid s$ then $a^s \equiv 1 \bmod p$ and $\gcd(a^s - 1, m)$ should contain p.

In fact, it is sufficient to have $\mathrm{ord}_p(a) \mid s$.

($\mathrm{ord}_p(a)$: order of a in $\mathbb{F}_p^*$)

Note on the choice of s:

Given B then s can be any smooth number, i.e., a number with many small factors which are less than B.

If gcd is 1 then try a different a, could increase s (= increase B)

But: too large values for s can yield m as gcd!

The method fails if all divisors of m are "strong primes", i.e., primes q such that $q-1$ has a factor $> B$.

2) Lenstra's Elliptic Curve Method (ECM)

Replace computations in $\mathbb{F}_p^*$ by computations on an Edwards curve mod p.

Consider a point P on $E_d: x^2 + y^2 = 1 + dx^2y^2$

If P has order r in the group $E_d(\mathbb{F}_p)$, then $[r]P = \underbrace{P + \ldots + P}_{r \text{ times}} = (0,1)$.

i.e. p divides the x-coordinate $x([r]P)$ of $[r]P$.

Hope that r is smooth (many small divisors) then choose again $s = \mathrm{Lcm}(1, \ldots, B_1)$ and compute

$$\gcd(x([s]P), m)$$

This reveals a factor p of m if $[s]P = (0,1)$ on $E_d(\mathbb{F}_p)$, i.e., if $\mathrm{ord}(P)_p \mid s$.

Algo →

Note that the computations are carried out for the curve E_d modulo m. Since m is composite (we're hoping for a divisor!) not all operations are well-defined. $\mathbb{Z}/m\mathbb{Z}$ is not a field!

However, if we encounter an impossible operation (division by 0) this gives a factor of m!

Algo Given m and a bound B.

1. Compute $s = \mathrm{lcm}(\{1, \ldots, B\})$
2. Choose d uniformly at random ($d \neq 0, d \neq 1$)
3. Compute a random point P on E_d.
4. Compute $d = \gcd(x([s]P), m)$.
5. If $d \neq 1$ return d.
6. Else go back to 2.

Recall:

Divisions mod m are done using the Extended Euclidean Algorithm.
Dividing by some b mod m means computing xgcd(b, m). Division fails if gcd(b, m) ≠ 1 → but this yields a factor of m!

For the purpose of ECM pretend to work over a field when calculating mod m. If an error occurs → factor.

Main goal: compute [s]P and hope for s to be a multiple of the order of P modulo p.

Order of an elliptic curve

The number of points on $E_d(\mathbb{F}_q)$ for some field $\mathbb{F}_q$ is bounded (

$$q+1-2\sqrt{q} \leq \#E_{(d)}(\mathbb{F}_q) \leq q+1+2\sqrt{q}.$$

For a fixed prime q many integer values ℓ are attained by varying (d) in the interval

Vary q and d → all values can be attained.

The running time of ECM depends on the probability that for a fixed prime p and a choice of B the curve E_d has group order $\#E_d(\mathbb{F}_p)$ not divisible by any prime $> B$.

If $\#E_d(\mathbb{F}_p)$ is not smooth with respect to B $\rightarrow$ choose a new curve (a new value d).

No prime p has a chance of escaping ECM!
Some value in the Hasse interval
$[p+1-2\sqrt{p},\ p+1+2\sqrt{p}]$
will be smooth.

For the purposes of cyphographic applications, think of index calculus where we look for integers factoring over a small factor base.

Running time of ECM depends on the probability that for a fixed p and a choice of B the curve E_d has an order which is divisible by a prime $> B$.

Exercises *

1) Use the $p-1$ method with $s = 840$ and try to factor $n = 53467$ using

(i) $a = 2$
(ii) $a = 3$ as a base

2) For the following pairs B and p find the fraction of integers in the interval $[p+1-2\sqrt{p},\ p+1+2\sqrt{p}]$ which have no prime divisors greater than B.

(a) $p = 109$, $B = 3$
(b) $p = 109$, $B = 17$
(c) $p = 1009$, $B = 19$

Use a computer if necessary.

* just for the fun.

Koblitz, A course in NT & Cryptography has more exercises and answers.

Merry XMAS!