RSA V

$p-1, p+1$ methods and ECM

Tanja Lange
(some slides joint work with Daniel J. Bernstein)

Eindhoven University of Technology

2MMC10 – Cryptology

$p-1$ method

Let $s = 232792560 = \text{lcm}(1, 2, 3, 4, 5, \ldots, 20)$.
Then $2^s - 1$ is divisible by

- 70 of the 168 primes $\leq 10^3$;
- 156 of the 1229 primes $\leq 10^4$;
- 296 of the 9592 primes $\leq 10^5$;
- 470 of the 78498 primes $\leq 10^6$; etc.

$p-1$ method

Let $s = 232792560 = \text{lcm}(1, 2, 3, 4, 5, \ldots, 20)$.
Then $2^s - 1$ is divisible by

- 70 of the 168 primes $\leq 10^3$;
- 156 of the 1229 primes $\leq 10^4$;
- 296 of the 9592 primes $\leq 10^5$;
- 470 of the 78498 primes $\leq 10^6$; etc.

We know from Fermat's little theorem that

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

for p prime and $\gcd(a, p) = 1$. If p is a factor of m then p divides

$$\gcd(a^{p-1} - 1, m).$$

$p-1$ method

Let $s = 232792560 = \text{lcm}(1, 2, 3, 4, 5, \ldots, 20)$.
Then $2^s - 1$ is divisible by

- 70 of the 168 primes $\leq 10^3$;
- 156 of the 1229 primes $\leq 10^4$;
- 296 of the 9592 primes $\leq 10^5$;
- 470 of the 78498 primes $\leq 10^6$; etc.

We know from Fermat's little theorem that

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

for p prime and $\gcd(a, p) = 1$. If p is a factor of m then p divides

$$\gcd(a^{p-1} - 1, m).$$

To find p, compute $\gcd(a^s - 1, m)$ for s with many small prime factors.

$p-1$ method

Let $s = 232792560 = \text{lcm}(1, 2, 3, 4, 5, \ldots, 20)$.
Then $2^s - 1$ is divisible by

- 70 of the 168 primes $\leq 10^3$;
- 156 of the 1229 primes $\leq 10^4$;
- 296 of the 9592 primes $\leq 10^5$;
- 470 of the 78498 primes $\leq 10^6$; etc.

We know from Fermat's little theorem that

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

for p prime and $\gcd(a, p) = 1$. If p is a factor of m then p divides

$$\gcd(a^{p-1} - 1, m).$$

To find p, compute $\gcd(a^s - 1, m)$ for s with many small prime factors.
Also need prime $q|m$ with $a^s - 1 \not\equiv 0 \bmod q$, else $\gcd(a^s - 1, m) = m$.

$p - 1$ method

Let $s = 232792560 = \text{lcm}(1, 2, 3, 4, 5, \ldots, 20)$.
Then $2^s - 1$ is divisible by

- 70 of the 168 primes $\leq 10^3$;
- 156 of the 1229 primes $\leq 10^4$;
- 296 of the 9592 primes $\leq 10^5$;
- 470 of the 78498 primes $\leq 10^6$; etc.

We know from Fermat's little theorem that

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

for p prime and $\gcd(a, p) = 1$. If p is a factor of m then p divides

$$\gcd(a^{p-1} - 1, m).$$

To find p, compute $\gcd(a^s - 1, m)$ for s with many small prime factors.
Also need prime $q | m$ with $a^s - 1 \not\equiv 0 \bmod q$, else $\gcd(a^s - 1, m) = m$.
Odd prime p divides $a^s - 1$ if and only if the order of a in $\mathbf{F}_p^*$ divides s.
The latter works for sure if $p - 1$ divides s, but this is not required.

$p-1$ method in practice

Put $s = \text{lcm}(2, 3, \ldots, B_1)$ for some B_1. Pick random a. Compute

$$b \equiv a^s \bmod m \text{ and } \gcd(b-1, m)$$

using fast exponentiation with reduction modulo m. s used repeatedly, so worth it computing a good addition chain. At least use sliding windows.

$p-1$ method in practice

Put $s = \text{lcm}(2, 3, \ldots, B_1)$ for some B_1. Pick random a. Compute

$$b \equiv a^s \bmod m \text{ and } \gcd(b-1, m)$$

using fast exponentiation with reduction modulo m. s used repeatedly, so worth it computing a good addition chain. At least use sliding windows.

We can reduce modulo m because computing $\gcd(a^s - 1, m)$ reduces modulo m in the first step, so keep numbers $< m$ in the exponentiation.

$p-1$ method in practice

Put $s = \text{lcm}(2, 3, \ldots, B_1)$ for some B_1. Pick random a. Compute

$$b \equiv a^s \bmod m \text{ and } \gcd(b-1, m)$$

using fast exponentiation with reduction modulo m. s used repeatedly, so worth it computing a good addition chain. At least use sliding windows.

We can reduce modulo m because computing $\gcd(a^s - 1, m)$ reduces modulo m in the first step, so keep numbers $< m$ in the exponentiation.

"Real" $p-1$ computations have a second stage in which one computes $\gcd((b^{q_1}-1)(b^{q_2}-1)(b^{q_3}-1)\cdots(b^{q_k}-1), m)$ for mall primes $B_1 < q_1, \ldots, q_k \leq B_2$. Several tricks for speed, not exactly this formula. Succeeds if order of a mod p divides sq_i for some $1 \leq i \leq k$.

$p-1$ method in practice

Put $s = \text{lcm}(2, 3, \ldots, B_1)$ for some B_1. Pick random a. Compute

$$b \equiv a^s \bmod m \text{ and } \gcd(b-1, m)$$

using fast exponentiation with reduction modulo m. s used repeatedly, so worth it computing a good addition chain. At least use sliding windows.

We can reduce modulo m because computing $\gcd(a^s - 1, m)$ reduces modulo m in the first step, so keep numbers $< m$ in the exponentiation.

"Real" $p-1$ computations have a second stage in which one computes $\gcd((b^{q_1}-1)(b^{q_2}-1)(b^{q_3}-1)\cdots(b^{q_k}-1), m)$ for mall primes $B_1 < q_1, \ldots, q_k \leq B_2$. Several tricks for speed, not exactly this formula.
Succeeds if order of a mod p divides sq_i for some $1 \leq i \leq k$.

Numbers are easy to factor if a factor p has smooth $p-1$.

"Safe primes", i.e., primes of the form $2p' + 1$, for p' a prime, are harder to factor

$p-1$ method in practice

Put $s = \text{lcm}(2, 3, \ldots, B_1)$ for some B_1. Pick random a. Compute

$$b \equiv a^s \bmod m \text{ and } \gcd(b-1, m)$$

using fast exponentiation with reduction modulo m. s used repeatedly, so worth it computing a good addition chain. At least use sliding windows.

We can reduce modulo m because computing $\gcd(a^s - 1, m)$ reduces modulo m in the first step, so keep numbers $< m$ in the exponentiation.

"Real" $p-1$ computations have a second stage in which one computes $\gcd((b^{q_1}-1)(b^{q_2}-1)(b^{q_3}-1)\cdots(b^{q_k}-1), m)$ for mall primes $B_1 < q_1, \ldots, q_k \leq B_2$. Several tricks for speed, not exactly this formula.
Succeeds if order of a mod p divides sq_i for some $1 \leq i \leq k$.

Numbers are easy to factor if a factor p has smooth $p-1$.

"Safe primes", i.e., primes of the form $2p'+1$, for p' a prime, are harder to factor with the $p-1$ method.
This does not help against the NFS nor against $p+1$ and ECM.

The $p + 1$ factorization method

Let $s = 232792560 = \text{lcm}(1, 2, 3, 4, 5, \ldots, 20)$ and $P = (3/5, 4/5)$ in the group $\text{Clock}(\mathbf{Q})$. Define $(X, Y) = sP \in \mathbf{Q} \times \mathbf{Q}$.

The integer $S_2 = 5^{232792560} X$ is divisible by
82 of the primes $\leq 10^3$;
223 of the primes $\leq 10^4$;
455 of the primes $\leq 10^5$;
720 of the primes $\leq 10^6$;
etc. For those primes, $(X, Y) = (0, \pm 1)$ on $\text{Clock}(\mathbf{F}_p)$.

The $p+1$ factorization method

Let $s = 232792560 = \text{lcm}(1, 2, 3, 4, 5, \dots, 20)$ and $P = (3/5, 4/5)$ in the group $\text{Clock}(\mathbf{Q})$. Define $(X, Y) = sP \in \mathbf{Q} \times \mathbf{Q}$.

The integer $S_2 = 5^{232792560} X$ is divisible by
82 of the primes $\leq 10^3$;
223 of the primes $\leq 10^4$;
455 of the primes $\leq 10^5$;
720 of the primes $\leq 10^6$;
etc. For those primes, $(X, Y) = (0, \pm 1)$ on $\text{Clock}(\mathbf{F}_p)$.

Given an integer m, compute $S_2 \equiv 5^s x(sP) \bmod m$ and $\gcd(S_2, m)$ hoping to factor m. Many p's not found by $\mathbf{F}_p^*$ are found by $\text{Clock}(\mathbf{F}_p)$.

The $p+1$ method changes from computing in $\mathbf{F}_p^*$, thus succeeding when $\text{ord}_p(a)$ divides s, to working in $\text{Clock}(\mathbf{F}_p)$, thus succeeding when $\text{ord}_p(P)$ divides $2s$.

$\text{ord}_p(a)$: order of a mod p in $\mathbf{F}_p^*$; $\text{ord}_p(P)$: order of P in $\text{Clock}(\mathbf{F}_p)$.

The $p+1$ factorization method

Let $s = 232792560 = \text{lcm}(1, 2, 3, 4, 5, \ldots, 20)$ and $P = (3/5, 4/5)$ in the group Clock($\mathbf{Q}$). Define $(X, Y) = sP \in \mathbf{Q} \times \mathbf{Q}$.

The integer $S_2 = 5^{232792560}X$ is divisible by
82 of the primes $\leq 10^3$;
223 of the primes $\leq 10^4$;
455 of the primes $\leq 10^5$;
720 of the primes $\leq 10^6$;
etc. For those primes, $(X, Y) = (0, \pm 1)$ on Clock($\mathbf{F}_p$).

Given an integer m, compute $S_2 \equiv 5^s x(sP) \bmod m$ and $\gcd(S_2, m)$ hoping to factor m. Many p's not found by $\mathbf{F}_p^*$ are found by Clock($\mathbf{F}_p$).

The $p+1$ method changes from computing in $\mathbf{F}_p^*$, thus succeeding when $\text{ord}_p(a)$ divides s, to working in Clock($\mathbf{F}_p$), thus succeeding when $\text{ord}_p(P)$ divides $2s$.

$\text{ord}_p(a)$: order of a mod p in $\mathbf{F}_p^*$; $\text{ord}_p(P)$: order of P in Clock($\mathbf{F}_p$).

If $p \equiv 3 \bmod 4$ and $p+1$ divides 232792560 then $5^{232792560}X \equiv 0 \bmod p$.
Proof: There are $p+1$ points in Clock($\mathbf{F}_p$) for $p \equiv 3 \bmod 4$.

The $p+1$ method succeeds if $p+1$ divides s.

The elliptic-curve method (ECM)

Pick curve E. Fix bounds B_1, B_2. Put $s = \text{lcm}(2, 3, \ldots, B_1)$.

Stage 1:
Pick point P on E over $\mathbf{Z}/m$, compute $R = sP$.

Stage 2:
For small primes $B_1 < q_1, \ldots, q_k \leq B_2$ compute $R_i = q_i R$.

Compute $\gcd\left(\prod x(R_i), m\right)$.

The elliptic-curve method (ECM)

Pick curve E. Fix bounds B_1, B_2. Put $s = \text{lcm}(2, 3, \ldots, B_1)$.

Stage 1:
Pick point P on E over $\mathbf{Z}/m$, compute $R = sP$.

Stage 2:
For small primes $B_1 < q_1, \ldots, q_k \leq B_2$ compute $R_i = q_i R$.

Compute $\gcd\left(\prod x(R_i), m\right)$.

If order of P in $E/\mathbf{F}_p$ (same curve, reduce mod p) divides some sq_i, then modulo p we have $R_i = (0, 1)$ (using Edwards).

The elliptic-curve method (ECM)

Pick curve E. Fix bounds B_1, B_2. Put $s = \mathrm{lcm}(2, 3, \ldots, B_1)$.

Stage 1:
Pick point P on E over $\mathbf{Z}/m$, compute $R = sP$.

Stage 2:
For small primes $B_1 < q_1, \ldots, q_k \leq B_2$ compute $R_i = q_i R$.

Compute $\gcd\left(\prod x(R_i), m\right)$.

If order of P in $E/\mathbf{F}_p$ (same curve, reduce mod p) divides some sq_i, then modulo p we have $R_i = (0, 1)$ (using Edwards).

ECM permits varying the curve. If a curve fails, try another.
$|E(\mathbf{F}_p)| \in [p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}]$.
All primes $\leq H$ found after reasonable number of curves.

The elliptic-curve method (ECM)

Pick curve E. Fix bounds B_1, B_2. Put $s = \mathrm{lcm}(2, 3, \ldots, B_1)$.

Stage 1:
Pick point P on E over $\mathbf{Z}/m$, compute $R = sP$.

Stage 2:
For small primes $B_1 < q_1, \ldots, q_k \leq B_2$ compute $R_i = q_i R$.

Compute $\gcd\left(\prod x(R_i), m\right)$.

If order of P in $E/\mathbf{F}_p$ (same curve, reduce mod p) divides some sq_i, then modulo p we have $R_i = (0, 1)$ (using Edwards).

ECM permits varying the curve. If a curve fails, try another.
$|E(\mathbf{F}_p)| \in [p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}]$.
All primes $\leq H$ found after reasonable number of curves.

Plausible conjecture: if B_1 is $\exp\sqrt{\left(\frac{1}{2} + o(1)\right)\log H \log\log H}$ then, for each prime $p \leq H$, a uniform random curve mod p has chance $\geq 1/B_1^{1+o(1)}$ to find p.
Find p using, $\leq B_1^{1+o(1)}$ curves; $\leq B_1^{2+o(1)}$ squarings. Time subexponential in H.

The elliptic-curve method (ECM)

Pick curve E. Fix bounds B_1, B_2. Put $s = \text{lcm}(2, 3, \ldots, B_1)$.

Stage 1:
Pick point P on E over $\mathbf{Z}/m$, compute $R = sP$.

Actually need to generate point along with curve;
cannot compute square roots modulo m.

Stage 2:
For small primes $B_1 < q_1, \ldots, q_k \leq B_2$ compute $R_i = q_i R$.

Compute $\gcd\left(\prod x(R_i), m\right)$.

If order of P in $E/\mathbf{F}_p$ (same curve, reduce mod p) divides some sq_i,
then modulo p we have $R_i = (0, 1)$ (using Edwards).

ECM permits varying the curve. If a curve fails, try another.
$|E(\mathbf{F}_p)| \in [p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}]$.
All primes $\leq H$ found after reasonable number of curves.

Fastest method
we have seen so far.

Plausible conjecture: if B_1 is $\exp\sqrt{\left(\frac{1}{2} + o(1)\right)\log H \log\log H}$ then, for each prime $p \leq H$, a uniform random curve mod p has chance $\geq 1/B_1^{1+o(1)}$ to find p.
Find p using, $\leq B_1^{1+o(1)}$ curves; $\leq B_1^{2+o(1)}$ squarings. Time subexponential in H.