Summer School - Number Theory for Cryptography

F. Morain

Tutorial, 2013/06/26

1. a) Program the $p-1$ method, together with its standard continuation.

b) Program Brent's continuation.

c) Let us describe a Baby-Step-Giant-Step continuation. Select $w \approx \sqrt{B_2}$, $v_1 = \lceil B_1/w \rceil$, $v_2 = \lceil B_2/w \rceil$. Write our prime s as $s = vw - u$, with $0 \leq u < w$, $v_1 \leq v \leq v_2$. Using the fact that $\gcd(b^s - 1, N) > 1$ iff $\gcd(b^{wv} - b^u, N) > 1$, give an algorithm to perform the search for s in $O(\sqrt{B_2})$ operations. Implement it and compare it to the continuations already given.

2. Let $p = 2k+1$ and $q = 4k+1$ be prime (with $k \geq 5$) and $N = pq$. Show that for all a prime to N, one has $\gcd(a^{k!} - 1, N) = N$. Show how to modify the $p-1$ method of factoring to recover p and q in that special case.

3. Give parametrizations of elliptic curves over $\mathbb{Q}$ having a 2-torsion point, respectively torsion subgroup of order 4, in Weierstrass or Edwards form. Are they interesting to use in ECM?

4. Program ECM.

5. (a) Let $\omega = 2^s t$, with integers s and t, t odd. One considers the sequence $y_0 = 1$, $y_k = 2y_{k-1} \bmod \omega$. Let e be the order of 2 in $(\mathbb{Z}/t\mathbb{Z})^*$. Show that the length and tail of the iteration are respectively s and e.

(b) Let p be a prime and $f : \mathbb{Z}/p\mathbb{Z} \longrightarrow \mathbb{Z}/p\mathbb{Z}$ such that $f(x) = x^2$. Define (a_k) by $a_0 = a$ (where $a \not\equiv 0 \bmod p$) and $a_k = f(a_{k-1}) = a^{2^k} \bmod p$. Let $\omega = 2^s t$ be the order of a modulo p. Compute the cycle length and tail length of the cycle of the sequence (a_k). Numerical values: $p = 59$, $a = 2$. Is the function f suitable for the ρ method?

(c) Let K be a field, and u, v two non-zero elements of K. Show that if $u + 1/u = v + 1/v$, then $u = v$ or $u = 1/v$.

(d) Let $a \neq 1$, $a \in (\mathbb{Z}/p\mathbb{Z})^*$. Put $x_0 = a + 1/a$, $f(x) = x^2 - 2 \bmod p$, $x_k = f(x_{k-1})$. Hence, $x_k = a^{2^k} + a^{-2^k}$. Let $\omega = 2^s t$ be the ordre of a modulo p. Let (H) denote the assertion: "the equation $2^\ell \equiv -1 \bmod t$ has at least one solution". Prove that if (H) is satisfied, the length of the cycle of (x_k) is $e/2$; otherwise, this length is equal to e. Compute the tail length.

(e) Let $x_0 \in \mathbb{Z}/p\mathbb{Z}$. Assume there is no solution to $x_0 = a + 1/a$ for $a \in (\mathbb{Z}/p\mathbb{Z})^*$. Let $\alpha \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ such that $x_0 = \alpha + 1/\alpha$. Let $\omega = 2^s t$ be the ordre of α in $\mathbb{F}_{p^2}$ and e the ordre of 2 modulo t. Show that α, α^2, ..., α^{2^s} are all distinct in $\mathbb{F}_{p^2}$ and that $\alpha^{2^{s+e}} = \alpha^{2^s}$. Define $x_k = f(x_{k-1})$ with $f(x) = x^2 - 2 \pmod p$. Show that if (H) is true, the cycle length is $e/2$ and e otherwise. Compute the tail length. Numerical values: $p = 5$, $x_0 = 1$.

(f) What happens if one uses $f(x) = x^2 - 2$ in the ρ method?