Mastermath Elliptic Curves, Homework set 11

Marco Streng and Martin Bright

Deadline: 1 December 2015, 10:15.

All non-optional problems and their solutions are part of the course and could play a role in the exam. Only problems 63, 65, 67 and 69 are to be handed in.

In these problems, let

$$\mathbf{P}^2(\mathbf{Z}/N\mathbf{Z}) = \{(a,b,c) \in (\mathbf{Z}/N\mathbf{Z})^3 : \gcd(a,b,c,N) = 1\}/\sim,$$

where $\sim$ is given by

$$(a:b:c) = (a':b':c') \quad \Leftrightarrow \quad \exists \lambda \in (\mathbf{Z}/N\mathbf{Z})^* : (a,b,c) = \lambda(a',b',c').$$

Problem 63. Use Pollard's $p-1$ method to find a non-trivial factor of the number $N = 5802023111$. You may use a computer for basic arithmetic in $\mathbf{Z}/N\mathbf{Z}$ and for computing the greatest common divisor. Do tell us all the steps of your computation.

We recommend using SageMath, Pari/GP or Magma, but we expect this to work also in Python, Maple, Mathematica or Wolfram Alpha:

`http://www.wolframalpha.com/input/?i=5^3+modulo+123`

`http://www.wolframalpha.com/input/?i=gcd(10,6)`

Warning: it is very easy and natural to program this algorithm in a spreadsheet, but a spreadsheet program (and all other programs that use floating point numbers or fixed-precision 'int's) will run into precision loss because of rounding or overflows, so this will not work.

Remark: this works very well with the version of the $p-1$ method from [HPS] or the lecture.

Problem 64. Let $p \neq 2$ be a prime and let $k = \mathbf{F}_p$. Let E/k be the elliptic curve in $\mathbf{P}^2$ given by $y^2 = f(x)$ and $O = (0:1:0)$, where $f(x) = ax^3 + bx^2 + cx + d$ is such that E is smooth. Given $e \in k^*$, let $E^{(e)}$ be given by $y^2 = ef(x)$.

(a) Show that if e is not a square in k^*, then $\#E(k) + \#E^{(e)}(k) = 2(p+1)$.

(b) Show that E and $E^{(e)}$ are isomorphic over $k(\sqrt{e})$, where $k(\sqrt{e}) = k$ if e is square. We call $E^{(e)}$ a *twist* of E.

Problem 65. Let $\mathbf{F}_5$ be a field with 5 elements.

(a) Show that for every elliptic curve $E/\mathbf{F}_5$, we have $2 \leq \#E(\mathbf{F}_5) \leq 10$.

(b) Give three elliptic curves over $\mathbf{F}_5$ with distinct numbers of points.

(c) (Optional: more work) Give for every integer n with $2 \leq n \leq 10$ an elliptic curve over $\mathbf{F}_5$ with exactly n points over $\mathbf{F}_5$.

Problem 66. For a group G and $g, h \in G$ as follows, determine $\log_g(h)$. You may use a computer or calculator *only* for $+$, $-$, $\times$ and $\div$. Explain how you got your answer. Say something sensible about the running time of your algorithm as the input gets larger.

(a) $G = \mathbf{C}^*$, $g = 10$, $h = 100000000000000000000000000000000000000000$,

(b) $G = \mathbf{Z}/1018\mathbf{Z}$ (additive!), $g = 629$, $h = 337$,

(c) $G = (\mathbf{Z}/11\mathbf{Z})^*$, $g = 7$, $h = 3$,

(d) $G = E(\mathbf{F}_7)$, where $E : y^2 = x^3 + x + 1$, $g = (0, 1)$, $h = (2, 2)$.

Problem 67. For G, g, g_a, g_b as below, suppose that Alice and Bob do a Diffie-Hellman key exchange with the group G and parameter $g \in G$, and that they send g_a and g_b to each other as part of the protocol. Break the cryptography by computing the element $g_{ab} \in G$ that determines the public key. You may use a computer or calculator *only* for $+$, $-$, $\times$ and $\div$. Explain how you got your answer. Say something sensible about the running time of your algorithm, including the algorithm for the relevant parts of Problem 66, as the input gets larger.

(a) G, g as in Problem 66.(b), $g_a = 337$, $g_b = 123$.

(b) G, g as in Problem 66.(c), $g_a = 3$ and $g_b = 5$,

Problem 68. Let $N \in \mathbf{Z}$ be a positive integer and $F \in \mathbf{Z}[X, Y, Z]$ a homogeneous polynomial such that $\overline{F} = (F \bmod N)$ is non-zero. Let C be the plane curve over $\mathbf{Q}$ given by the equation $F = 0$, and let $C(\mathbf{Z}/N\mathbf{Z})$ be the set of points $(X : Y : Z) \in \mathbf{P}^2(\mathbf{Z}/N\mathbf{Z})$ satisfying $\overline{F}(X, Y, Z) = 0$.

(a) Give a natural map $f : C(\mathbf{Q}) \to C(\mathbf{Z}/N\mathbf{Z})$.

(b) Give an example where f is not surjective.

(c) Give an example where f is not injective.

(d) Suppose $N = N_1 N_2$ with $\gcd(N_1, N_2) = 1$. Give a natural bijection

$$C(\mathbf{Z}/N\mathbf{Z}) \leftrightarrow C(\mathbf{Z}/N_1\mathbf{Z}) \times C(\mathbf{Z}/N_2\mathbf{Z}).$$

(e) Show that the line $Y = 0$ intersects the elliptic curve $F : Y^2 = X^3 - X$ in nine points of $F(\mathbf{Z}/15\mathbf{Z})$, not counted with multiplicity.
Conclude that one cannot straightforwardly use intersection with a line to compute $P + Q$ for $P = (1, 0)$ and $Q = (2, 0) \in F(\mathbf{Z}/15\mathbf{Z})$.

Let E be an elliptic curve over $\mathbf{Z}/N\mathbf{Z}$, that is, a projective plane Weierstrass equation over $\mathbf{Z}/N\mathbf{Z}$ with discriminant in $(\mathbf{Z}/N\mathbf{Z})^*$. Let $r(N)$ be the radical of N, i.e., the product of the primes dividing N. Let $\phi : E(\mathbf{Z}/N\mathbf{Z}) \to \prod_{p|N} E(\mathbf{Z}/p\mathbf{Z})$ be the natural map, where the product is taken over primes dividing N.

(f) Show that, given any pair of points $P, Q \in E(\mathbf{Z}/N\mathbf{Z})$, the addition formula (e.g. Problem 12) allows you to compute either

(i) $R \in E(\mathbf{Z}/N\mathbf{Z})$ with $\phi(R) = \phi(P) + \phi(Q)$ or

(ii) a divisor $d \mid N$ with $d \neq 1, N$.

(g) Try out the method of (f) for some choices of points $P, Q \in F(\mathbf{Z}/15\mathbf{Z})$ with $Y = 0$. What happens? Give a point R with $\phi(R) = \phi(P) + \phi(Q)$.

In fact, one can show that $E(\mathbf{Z}/N\mathbf{Z})$ is in a natural way a group, but we will not do that at this point, and it is not needed for the algorithms of this week.

Problem 69. Let E be the elliptic curve over $\mathbf{Z}/9\mathbf{Z}$ given by $E : Y^2Z = X^3 + 7XZ^2$. You may use that $E(\mathbf{Z}/9\mathbf{Z}) \subset \mathbf{P}^2(\mathbf{Z}/9\mathbf{Z})$ is a group and that $\pi : E(\mathbf{Z}/9\mathbf{Z}) \to E(\mathbf{Z}/3\mathbf{Z})$ is a homomorphism.

(a) Determine the order of the group $E(\mathbf{Z}/3\mathbf{Z})$, show that it is cyclic, and give a generator.

(b) Determine the order of the kernel of π, show that it is cyclic, and give a generator.

(c) Is π surjective?

(d) Determine the order of the group $E(\mathbf{Z}/9\mathbf{Z})$ and give a generating set. Is the group cyclic?

Problem 70. In this exercise, you use elliptic curves to prove that a number is prime.

(a) Let E be an elliptic curve over $(\mathbf{Z}/N\mathbf{Z})$, let $P \in E(\mathbf{Z}/N\mathbf{Z})$ and let m and q be positive integers such that q divides m. Suppose that

(i) $[m/q]P = (x : y : z)$ with $z \in (\mathbf{Z}/N\mathbf{Z})^*$,

(ii) $[m]P = (0 : 1 : 0)$, and

(iii) $q > (\sqrt[4]{N} + 1)^2$.

Prove that we have

$$q \text{ is prime} \quad \Longrightarrow \quad N \text{ is prime.}$$

Let the integers n_i, m_i, elliptic curves E_i over $(\mathbf{Z}/n_i\mathbf{Z})$ and points $P_i \in E_i(\mathbf{Z}/n_i\mathbf{Z})$ be as follows.

$n_1 = 220307,$	$E_1 : y^2 = x^3 - 4x^2 - 48x - 64,$	$P_1 = (179428 : 175886 : 1),$	$m_1 = 66,$
$n_2 = 3329,$	$E_2 : y^2 = x^3 + 3x,$	$P_2 = (1646 : 1410 : 1),$	$m_2 = 17,$
$n_3 = 101.$			

For all $i \in \{1, 2\}$, we have $[m_i]P_i = (x : y : z)$ with $z \in (\mathbf{Z}/n_i\mathbf{Z})^*$ and $[n_{i+1}m_i]P_i = (0 : 1 : 0)$.

(b) (Optional: requires SageMath.) Check this.

(c) Use this information to prove that 220307 is prime.

Problem 71. (Optional: for those who have done Problem 15.) What can you say about the safety of elliptic curve cryptography on singular Weierstrass curves? Note that there are two cases: $\overline{k}^*$ and $(k, +)$.

Problem 72. (Optional) What can you say about the discrete logarithm problem on elliptic curves over $\mathbf{Q}$? Hint: use the height.