Elliptic curves: homework 13
Mastermath / DIAMANT, Spring 2019
Martin Bright and Marco Streng

1. 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 $\div$. Say something sensible about the running time of your algorithm as the input gets larger.

(a) $G = \mathbb{C}^*$, $g = 10$, $h = 1000000000000000000000000000000000000$,
(b) $G = \mathbb{Z}/1018\mathbb{Z}$ (additive!), $g = 629$, $h = 337$,
(c) $G = (\mathbb{Z}/11\mathbb{Z})^*$, $g = 7$, $h = 3$,
(d) $G = E(\mathbb{F}_7)$, where $E : y^2 = x^3 + x + 1$, $g = (0, 1)$, $h = (2, 2)$.

2. What can you say about the discrete logarithm problem on elliptic curves over $\mathbb{Q}$? Hint: use the height.

3. 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 shared key. You may use a computer or calculator *only* for $+$, $-$, $\times$ and $\div$. Say something sensible about the running time of your algorithm, including the algorithm for the relevant parts of Problem 1, as the input gets larger.

(a) G, g as in Problem 1(1b), $g_a = 337$, $g_b = 123$.
(b) G, g as in Problem 1(1c), $g_a = 3$ and $g_b = 5$,

4. 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 $\mathbb{Z}/N\mathbb{Z}$ and for computing the greatest common divisor.

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 the lecture or the book of Hoffstein, Pipher and Silverman.

In the following problems, let

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

where $\sim$ is given by

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

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

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

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

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

(d) Suppose $N = N_1N_2$ with $\gcd(N_1, N_2) = 1$. Give a natural bijection

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

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

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

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

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

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

(b) Try out the method of (5a) for some choices of points $P, Q \in F(\mathbb{Z}/15\mathbb{Z})$ with $Y = 0$. What happens? Give a point R with $\phi(R) = \phi(P) + \phi(Q)$.

In fact, one can show that $E(\mathbb{Z}/N\mathbb{Z})$ 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.

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

(a) Determine the order of the group $E(\mathbb{Z}/3\mathbb{Z})$, 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 $E(\mathbb{Z}/9\mathbb{Z})$ and give a generating set. Is the group cyclic?