IV054
Solution of HW 8

1 Hashing and ElGamal signature

See the file signature.xls.

2 Hasse theorem for bounds of EC order; EC with the same order an different group structure

By Vincent Mihalkovič:

SageMath helps me a lot:

```
maxx, minn = 0, Integer.MAX_VALUE
for a in range(7):
    for b in range(7):
# We need to check non-singularity (-16(4a**3 + 27b**2) % 7 != 0)
        E = EllipticCurve(GF(7), [a,b])
        number_of_points = len( E.points() )
        if number_of_points < minn:
            minn = number_of_points
            min_curve = E
        if number_of_points > maxx:
            maxx = number_of_points
            max_curve = E
        if number_of_points == 9:
            print( E.abelian_group() )

print( min_curve, min_curve.points() )
print( max_curve, max_curve.points() )
```

(a) First, look at the Hasse's theorem on elliptic curves:

$$|N - p - 1| \leq 2\sqrt{p}$$
$$|N - 8| \leq 2\sqrt{8}$$
$$8 - 2\sqrt{8} \leq N \leq 8 + 2\sqrt{8}$$
$$3 \leq N \leq 13$$

Minimal curve $y^2 = x^3 + 4$ with 3 points:
$[\infty, (0,2), (0,5)]$
Maximum curve $y^2 = x^3 + 3$ with 13 points:
$[\infty, (1,2), (1,5), (2,2), (2,5), (3,3), (3,4), (4,2), (4,5), (5,3), (5,4), (6,3), (6,4)]$

(b) Additive Abelian group isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_3$ embedded in Abelian group of points on Elliptic Curve defined by $y^2 = x^3 + 2$ over $\mathbb{F}_7$
If we look at the points $([\infty, (0,3), (0,4), (3,1), (3,6), (5,1), (5,6), (6,1), (6,6)])$ All of them has order 3 (except ∞) there is **no** generator element with order 9.
But additive Abelian group isomorphic to $\mathbb{Z}_9$ embedded in Abelian group of points on Elliptic Curve defined by $y^2 = x^3 + 3x + 2$ over $\mathbb{F}_7$, has
$[\infty, (0,3), (0,4), (2,3), (2,4), (4,1), (4,6), (5,3), (5,4)]$ points, in which six of them
$[(2,3), (2,4), (4,1), \ldots]$ has order 9, thus they are generators of this Abelian group!

3 Proof of theorem and estimating bounds

By Jakub Dóczy:

(a) When considering, if $i \in \mathbb{Z}_p; (x = i, y)$ is a valid point on a curve, we have to evaluate $y^2 = x^3 + ax^2 + b$ and determine, if $x^3 + ax^2 + b$ is a quadratic residue. We have 3 possible outcomes.

(i) $x^3 + ax^2 + b = 0:$ (x, y) is a point on a curve.

(ii) $x^3 + ax^2 + b$ is a quadratic residue : $(x, y), (x, -y)$ are points on a curve (if p is a prime, we can always find two distinct points because $y \not\equiv -y \bmod p$ and $(-y)^2 = y^2$).

(iii) $x^3 + ax^2 + b$ is not a quadratic residue : there cannot exist any y, such that (x, y) is a point on this elliptic curve.

Since this lists all possible points (x, y) for any $x \in \mathbb{Z}_p$, we can count the number of points on elliptic curve E as:

$$|E| = 1 + \sum_{x=0}^{p-1} \begin{cases} 0 & \text{if } x^3 + ax^2 + b \text{ is not a quadratic residue} \\ 1 & \text{if } x^3 + ax^2 + b = 1 \\ 2 & \text{if } x^3 + ax^2 + b \text{ is a quadratic residue} \end{cases}$$

We have to add 1, because of the neutral element $(\mathcal{O})$.
And this equation is equivalent to:

$$|E| = 1 + \sum_{x=0}^{p-1} \left(\left(\frac{x^3 + ax^2 + b}{p} \right) + 1 \right) = 1 + p + \sum_{x=0}^{p-1} \left(\frac{x^3 + ax^2 + b}{p} \right)$$

(b) The number of points on elliptic curve is bound by Hesse's theorem

$$p - 2\sqrt{p} - 1 \leq N \leq p + 2\sqrt{p} + 1$$

Substituting N by equation from a) we get:

$$p - 2\sqrt{p} - 1 \leq 1 + p + \sum_{x=0}^{p-1} \left(\frac{x^3 + ax^2 + b}{p} \right) \leq p + 2\sqrt{p} + 1$$

$$-2\sqrt{p} \leq \sum_{x=0}^{p-1} \left(\frac{x^3 + ax^2 + b}{p} \right) \leq 2\sqrt{p}$$

$$\left| \sum_{x=0}^{p-1} \left(\frac{x^3 + ax^2 + b}{p} \right) \right| \leq 2\sqrt{p}$$

4 Factorization

By Daniel Schramm:

We know that the function $f(x) = 2^x \bmod 1927$ has a period $r = 460$.

To factorise the number 1927 we will perform a subroutine of the Shor's quantum polynomial time algorithm for integer factorisation.

First, we check whether $r = 460$ is an even number.

Obviously, r is an even number.
Therefore, we continue by checking if $2^{\frac{r}{2}} \equiv \pm 1 \pmod{1927}$.

Since $2^{\frac{460}{2}} \equiv 1270 \pmod{1927}$, we know that 1270 is a nontrivial solution of $x^2 \equiv 1 \pmod{1927}$.
This implies that $1927 \mid ((1270 - 1) \cdot (1270 + 1))$.

We compute the factors N_1, N_2 of 1927 as follows:

$$\begin{aligned} N_1 &= \gcd(1270 - 1, 1927) \\ &= 47 \end{aligned} \qquad\qquad \begin{aligned} N_2 &= \gcd(1270 + 1, 1927) \\ &= 41 \end{aligned}$$

The factors of the number 1927 are 41 and 47.

5 Finding order of EC using Hasse's theorem and Langrange's

By Markéta Naušová:

First we can use Hasse's theorem to get some bounds on the number of points on the elliptic curve E. From the assignment we have $p = 113$. The Hasse's theorem says that $||E| - p - 1| \leq 2\sqrt{p}$. We can modify the nonequality so that is says that $|E| \leq p + 2\sqrt{p} + 1$ and $|E| \geq p - 2\sqrt{p} + 1$.

$$|E| \geq 113 - 2\sqrt{113} + 1 \doteq 92,7$$
$$|E| \leq 113 + 2\sqrt{113} + 1 \doteq 135,3$$

Therefore we have the integer bounds $93 \leq |E| \leq 135$.

Let's denote the points on the curve from the assignment as $P = (74, 3)$ and $Q = (28, 11)$. Each point of the curve generates a cyclic subgroup. For example point P generates a subgroup of order 3 and point Q generates a subgroup of order 14 (the order is the number of points in the subgroup, so that is is the smallest positive integer k st $kP = 0$).

Lagrange's theorem says that if H is a subgroup of a finite group G, then the order of H divides the order of G.

We can use this theorem to find number of point of the curve E. We know that $(E, +)$ has subgroup generated by P with order 3 and another subgroup generated by Q with order 14. It must hold that 3|order of group formed by E and 14|order of group formed by E. Since order of group is the number of elements in the group we can write $3 \mid |E|$ and $14 \mid |E|$ (3 and 14 divide |E|). Hence we can say that $|E| = k \cdot 3$ for some integer k and also $|E| = l \cdot 14$ for some integer l. Together we can say that $|E| = m \cdot 3 \cdot 14 = m \cdot 42$ for some integer m. The only m for which also the condition $93 \leq |E| = m \cdot 42 \leq 135$ holds is $m = 3$, which gives us $|E| = 42 \cdot 3 = 126$. The number of points of E is therefore 126.

6 Discovering vulnerability of the established key

By Aleš Paroulek:

$n_A P = (55, 0)$

By definition of point addition, if we add two points P_1 and P_2 such that $P_1 = P_2$ and $y_1 = 0$, the lambda will have no solution and in such a case the result will be the infinity point.

Since Bob chose a number n_B which will multiply the point $n_A P$, the only possible keys are (55, 0) and the infinity point, since $(55, 0) + (55, 0) = \infty$ and $(55, 0) + \infty = (55, 0)$ and this would again repeat.