Fachbereich Mathematik
Elena Klimenko

WS 2017/18
Homework 11

NUMBER THEORY AND CRYPTOGRAPHY

Due in class on Friday, January 19th, at 12:05 pm.

1. Use Pollard's $p-1$ factorization algorithm to factor both of the following numbers:

(a) $n = 1739$ (b) $n = 220459$.

Be sure to show your work and to indicate which prime factor p has the property that $p-1$ is the product of small primes.

2. Apply the factorization procedure described in Section 20.1 of our lecture notes (also known as Dixon's factorization method) to factor $n = 52907$. You may use the following data:

$$\begin{aligned} 399^2 &\equiv 480 \pmod{52907} & 480 &= 2^5 \cdot 3 \cdot 5 \\ 763^2 &\equiv 192 \pmod{52907} & 192 &= 2^6 \cdot 3 \\ 773^2 &\equiv 15552 \pmod{52907} & 15552 &= 2^6 \cdot 3^5 \\ 976^2 &\equiv 250 \pmod{52907} & 250 &= 2 \cdot 5^3 \end{aligned}$$

3. Use Lenstra's elliptic curve factorization algorithm to factor the number

$$n = 589$$

using the elliptic curve

$$E: \ y^2 = x^3 + 4x + 9 \quad \text{and} \quad P = (2, 5) \in E.$$

Show how the algorithm works!

4. A *primitive Pythagorean triple* (or *PPT* for short) is a triple of positive integers (x, y, z) that are pairwise relatively prime and satisfy the equation $x^2 + y^2 = z^2$.

(a) Prove that for any PPT (x, y, z) the following holds:

- One of x and y is odd, the other is even.
- If x is odd, then there exist odd integers s and t, where $s > t > 0$ and $\gcd(s, t) = 1$, so that

$$x = st, \quad y = \frac{s^2 - t^2}{2}, \quad z = \frac{s^2 + t^2}{2}.$$

(b) Prove that the equation

$$a^4 + b^4 = c^2$$

has no solutions in positive integers.