Exercises for Chapter 4

Exercise 1 – [Carmichael function]

Let $N > 2$ be an odd number and let $N = \prod_{i=1}^{r} p_i^{e_i}$ be its decomposition into prime factors. We put

$$\lambda(N) = \mathrm{lcm}\Big(\phi(p_1^{e_1}), \ldots, \phi(p_r^{e_r})\Big),$$

where ϕ is Euler's totient function.

1. Prove that $a^{\lambda(n)} = 1$ for every $a \in \big(\mathbb{Z}/N\mathbb{Z}\big)^*$.

2. Prove that

$$\forall a \in (\mathbb{Z}/N\mathbb{Z})^*,\ a^{N-1} = 1 \Longleftrightarrow \lambda(N) \mid N-1.$$

3. Let

$$C_N = \{a \in (\mathbb{Z}/N\mathbb{Z})^*;\ a^{\lambda(N)/2} = \pm 1\}.$$

Prove that C_N is a multiplicative subgroup of $(\mathbb{Z}/N\mathbb{Z})^*$ and that

$$C_N = (\mathbb{Z}/N\mathbb{Z})^* \Longleftrightarrow N = p^e \ \text{ with } p \text{ prime and } e \geq 1.$$

Exercise 2 – [Lenstra's numbers]

We say that an integer $N > 1$ is a Lenstra number if and only if

$$a^{N+1} \equiv a \bmod N \quad \text{for every } a \in \mathbb{Z}.$$

For instance 2 and 6 are two Lenstra numbers.

1. Prove that N is a Lenstra number if and only if it is squarefree and $p - 1 \mid N$ for every prime divisor p of N.

2. Show that the set of Lenstra numbers is finite and give the complete list of its elements.

Exercise 3 – [Lehmann's test]

Here we study a probabilistic test due to Lehmann, which is a variant of

Solovay-Strassen algorithm. Let n be an odd integer ≥ 3. We denote by f the map from $(\mathbb{Z}/n\mathbb{Z})^*$ into $(\mathbb{Z}/n\mathbb{Z})^*$ defined by $f(a) = a^{(n-1)/2}$ and we put $E = f\left((\mathbb{Z}/n\mathbb{Z})^*\right)$.

1. Show that if n is prime $E = \{-1, 1\}$.

2. Show that if n is not a prime power $E \neq \{-1, 1\}$.

3. Show that if $n = p^k$ with p prime and $k \geq 2$ we have also $E \neq \{-1, 1\}$.

4. Show that if $E = \{1\}$, n is a Carmichael number.

5. Let us consider the following algorithm.

Algorithm 1. Lehmann's test

Require: n an odd integer and an integer $t > 0$ (number of trials).
Ensure: $F(n, t) =$ `Probably composite` or `Probably prime`

```
for i from 1 to t do
    Choose a_i ∈ [1, n − 1] uniformly at random.
    Compute b_i = a_i^{(n−1)/2} mod n.
if {b_1, ..., b_t} ≠ {−1, 1} then
    Return Probably composite.
Return Probably prime.
```

Show that, if n is prime, the probability that the algorithm returns `probably prime` is at least $1 - 2^{1-t}$. Moreover, show that, if n is composite, the probability that the algorithm returns `probably composite` is at least $1 - 2^{-t}$.

6. Show that the word complexity of this algorithm is in $\widetilde{O}\left(t(\log n)^2\right)$.

7. For each of the numbers 343, 561, 667 et 841, compute E and compute the exact value of the probability that the algorithm is wrong. Compare with the bounds of question **5**.

Exercise 4 – [Pepin's test]

We are interested here in Fermat numbers $F_n = 2^{2^n} + 1$ where $n \geq 0$. Fermat had remarked that $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ et $F_4 = 65537$ were prime and has asked the question of the primality of the following ones, but Euler established that $F_5 = 641 \times 6700417$.

Note. These numbers appear also in Gauss theorem on the constructibility (with rule and compas) of regular polygones: a regular polygone with n vertices is constructible if and only if n is a power of 2 or is the product of a power of 2 and of r Fermat numbers *prime and distinct*, i.e. $n = 2^k p_1 \dots p_r$ (with $k, r \geq 0$, $p_i \neq p_j$ if $i \neq j$ and p_i Fermat prime for every $1 \leq i \leq r$).

1. Show that if a number $N = 2^k + 1$ is prime, then k is a power of 2, so that N is a Fermat number.

2. Show that if F_n is prime with $n \geq 1$, neither 3 nor 7 are quadratic residues modulo F_n and that it is also the case for 5 if $n \geq 2$.

3. Suppose $n \geq 1$. Prove the following equivalence (Pepin's test):

$$F_n \text{ prime} \iff 3^{(F_n-1)/2} \equiv -1 \mod F_n.$$

4. Show that the word complexity of Pepin's test is in $\widetilde{O}(4^n)$.

5. Let $n \geq 2$. Show that if p prime divides F_n then 2^{n+2} divides $p-1$ (we refind Euler's example with $5 \cdot 2^7 + 1 = 641$).

Exercise 5 – [Lucas-Lehmer test for Mersenne numbers]

1. Show that if $2^n - 1$ is prime then necessarily n is prime.

2. A perfect number is an integer which is equal to the sum of its proper divisors. For instance $6 = 1 + 2 + 3$ is perfect. Prove that an even number n is perfect if and only if there exists a prime p with $2^p - 1$ prime and $n = 2^{p-1}(2^p - 1)$.

A *Mersenne number* is a number $M_p = 2^p - 1$ with p prime. These numbers have been deeply studied, in particular to find big primes and as a consequence big even perfect numbers. For instance, it has been discovered in 2006 that $M_{32582657}$ is prime. This integer has 9808358 decimal digits and the even perfect number that it generates has 19616714 decimal digits! The interest of the situation is that we have at our disposal an efficient algorithm for the primality of the M_p. This test is linked to the following result.
Define the sequence L_n in the following way:

$$L_0 = 4 \text{ and } L_{n+1} = L_n^2 - 2 \text{ for } n \geq 0.$$

Theorem (Lucas-Lehmer test). *Let $p \geq 3$ be a prime odd number. We have the following equivalence:*

$$M_p \text{ is prime} \iff M_p \mid L_{p-2}.$$

We want now to prove this theorem. First suppose that $M_p \mid L_{p-2}$.

3. Put $\omega = 2 + \sqrt{3}$ and $\overline{\omega} = 2 - \sqrt{3}$. Prove that for every n we have

$$L_n = \omega^{2^n} + \overline{\omega}^{2^n}.$$

4. Prove that if $M_p \mid L_{p-2}$, there exists an integer k such that

$$\omega^{2^{p-1}} = kM_p\omega^{2^{p-2}} - 1.$$

5. Suppose that M_p is not prime and consider q the smallest prime divisor of M_p. Then put

$$X = \{a + b\sqrt{3};\ a,\ b \in \mathbb{Z}/q\mathbb{Z}\},$$

a set on which we have a commutative and associative multiplication, whith neutral element 1, trivially defined by

$$(a + b\sqrt{3})(c + d\sqrt{3}) = (ac + 3bd) + (bc + ad)\sqrt{3},$$

where additions and multiplications in the right hand side are done in $\mathbb{Z}/q\mathbb{Z}$. Let X' the set of the invertible elements of X. Check that X' is a group containing ω, $\overline{\omega}$ with no more than $q^2 - 1$ elements.

6. Show with the help of question **4** that in X', ω has order 2^p.

7. Deduce from this a contradiction and conclude.

Suppose now that M_p is prime with $p \geq 3$.

8. Show that $3^{(M_p-1)/2} \equiv -1 \mod M_p$ and that $2^{(M_p-1)/2} \equiv 1 \mod M_p$.

9. Consider X' defined as above, but now with $q = M_p$. Put $\alpha = 2\sqrt{3}$. Show that in X' we have $(6 + \alpha)^{M_p} = 6 - \alpha$.

10. Seeing that $\omega = (6 + \alpha)^2/24$, show that in X' we have $\omega^{(M_p+1)/2} = -1$.

11. Deduce from this that $L_{p-2} = 0$ in X' and conclude.

12. Write the algorithm and give an estimation of its complexity.

Exercise 6 – [Pollard's $p - 1$ method]

Using Pollard's $p - 1$ algorithm, factor $N = 26869$ (take $a = 7$) and $N = 13861$ (take $a = 2$).

Exercise 7 – [Elliptic curves]

1. Consider the elliptic curve over $\mathbb{F}_7$ defined by the equation $y^2 = x^3 + x + 3$. Compute all points on it, and check that the elliptic curve group (the curve equiped with the standard addition and considered as an abelian group) is cyclic and generated by $(4, 1)$.

2. Let E be an elliptic curve over a field K. Show that if $\#E$ is a squarefree integer, then the elliptic curve group is cyclic.

3. Let $p > 2$ a prime and $E :\ y^2z = x^3 + axz^2 + bz^3$ an elliptic curve over $\mathbb{F}_p$. We write χ for the Legendre symbol $\left(\frac{\cdot}{p}\right)$. Prove that

$$\#E(\mathbb{F}_p) = p + 1 + \sum_{x \in \mathbb{F}_p} \chi(x^3 + ax + b)$$

and that this formula computes $\#E(\mathbb{F}_p)$ in time $\widetilde{O}(p)$.

4. With the same notation, let $g \in \mathbb{F}_p$ be a quadratic non-residue and let us consider the quadratic twist of E, $E' : gy^2z = x^3 + axz^2 + bz^3$. Prove that

$$\#E(\mathbb{F}_p) + \#E'(\mathbb{F}_p) = 2p + 2.$$

Exercise 8 – [Torsion points]

If $E(K)$ is an elliptic curve over a field K with neutral element O_E, we call torsion point of E every P such that $[n]P = O_E$ for a given $n > 0$ i.e. P is of finite order. We denote by $E(K)_t$ the set of the torsion points of $E(K)$.

1. Prove that $E(K)_t$ is an abelian group.

2. For $E(\mathbb{Q})$ defined by $y^2 = x^3 - 4x$ prove that $E(\mathbb{Q})_t \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

3. For $E(\mathbb{Q})$ defined by $y^2 = x^3 + 1$ prove that $E(\mathbb{Q})_t \simeq \mathbb{Z}/6\mathbb{Z}$.

4. For $E(\mathbb{Q})$ defined by $y^2 = x^3 - 432$ prove that $E(\mathbb{Q})_t \simeq \mathbb{Z}/3\mathbb{Z}$.

5. Find an elliptic curve over $\mathbb{Q}$ with no nontrivial torsion point.

Exercise 9 – [Complex multiplication]

1. Show that $K = \mathbb{Q}(\sqrt{-163})$ has trivial class group. Then explain why $\exp(\pi\sqrt{163})$ is very close to an integer.

2. Let E be an elliptic curve with complex multiplication by the imaginary quadratic order of discriminant D. Show that if p is a prime such that $\left(\frac{D}{p}\right) = -1$, then $\#E(\mathbb{Z}/p\mathbb{Z}) = p + 1$.

3. Show that the elliptic curve $y^2 = 4x^3 - 30x - 28$ has complex multiplication by $\mathbb{Z}[\sqrt{2}]$ and give explicitly the action of multiplication by $\sqrt{2}$ on a point (x, y).

Exercise 10 – [ECPP and Factoring with EC]

1. Using E with equation $y^2 = x^3 + 9x + 1$ and $P = (0, 1)$, prove that $N = 1231$ is prime.

2. Using E with equation $y^2 = x^3 + 3x + 4$ and $P = (0, 2)$, prove that $N = 1117$ is prime.

3. Prove that a Mersenne number $N = 2^p - 1$ (with p prime) is a prime if and only if there exists a point $P = (x, y)$ on the curve $E : y^2 = x^3 + x \bmod N$ such that

1. $2^{p-1}P$ can be computed without encountering non-invertible denominators mod N;

2. $2^{p-1}P$ has y-coordinate zero.

4. Using E with equation $y^2 = x^3 + ax + 4$ (where $a \in \mathbb{Z}_{\geq 0}$) and $P = (0, 2)$, factor $N = 899$.

5. Using E with equation $y^2 = x^3 + ax + 1$ (where $a \in \mathbb{Z}_{\geq 0}$) and $P = (0, 1)$, factor $N = 3551$.

Exercise 11 – [Sieving methods]

1. Show that if n is odd, composite, and not a power, then at least half of the pairs x, y with $0 \leq x, y < n$ and $x^2 \equiv y^2 \bmod n$ have $1 < \gcd(x - y, n) < n$.

2. As usually we denote by M_p the Mersenne number $2^p - 1$. Use the explicit congruences

$$\begin{cases} 258883717^2 \bmod M_{29} &= -2 \cdot 3 \cdot 5 \cdot 29^2, \\ 301036180^2 \bmod M_{29} &= -3 \cdot 5 \cdot 11 \cdot 79, \\ 126641959^2 \bmod M_{29} &= 2 \cdot 3^2 \cdot 11 \cdot 79, \end{cases}$$

to discover a factor of M_{29}.

3. Use the Quadratic Sieve algorithm to factor $N = 39617$.

4. As usually we denote by F_k the Fermat number $2^{2^k} + 1$. Show that

$$2^{3 \cdot 2^{k-2}} - 2^{2^{k-2}} \quad \text{and} \quad 2^{(p+1)/2}$$

are square roots of 2 respectively modulo F_k and modulo M_p (p odd).

5. Using question **3**, prove the congruence

$$2(2^6 - 8)^2 \equiv (2^6 + 1)^2 \bmod M_{11}$$

and infer from this the factorization of M_{11}.

Exercise 12 – [Pollard's original sieve method 1988]

Let $\alpha = (-2)^{1/3}$ an put $K = \mathbb{Q}(\alpha)$.

1. Show that $\mathbb{Z}_K = \mathbb{Z}[\alpha]$ and that this ring is a PID.

2. Show that for every $x \in \mathbb{Z}$, $N_{K/\mathbb{Q}}(x - \alpha) = x^3 + 2$ and that $2F_5$ is a norm of an element $\lambda \in \mathbb{Z}_K$.

3. Pollard's idea is to find an element $\beta \in \mathbb{Z}_K$ prime which divides λ. In this case we have

$$N_{K/\mathbb{Q}}(\beta) \mid N_{K/\mathbb{Q}}(\lambda)$$

and we may be able to find a nontrivial factor of F_5. For convenience, we look for $\beta = a + b\alpha \in \mathbb{Z}_K$ with $a, b \in \mathbb{Z}$ such that

$$\gcd(N_{K/\mathbb{Q}}(a + b\alpha), F_5) = \gcd(a^3 - 2b^3, F_5) > 1.$$

It is easy to see that $\beta = 16 + 5\alpha$ leads to the nontrivial divisor 641 of F_5. Using this method and a computer, find an odd nontrivial factor of the following given integers:

1. $2^{373} + 1$ (use $\mathbb{Z}[(-4)^{1/3}]$)
2. $2^{457} + 1$ (same hint)
3. $7^{149} + 1$ (use $\mathbb{Z}[(-7)^{1/3}]$)
4. $3^{239} - 1$ (use $\mathbb{Z}[3^{1/3}]$).