FINAL EXAM

1. (a) Describe the RSA public key cryptosystem. **(2 points)**

   (b) Alice establishes an RSA cryptosystem. Prove that if Eve knows that p, q are twin primes (i.e. $q = p + 2$), then she can easily break the cryptosystem, namely she can decrypt any cipher in polynomial time. **(4 points)**

Solution. (a) Alice takes two (large) prime numbers p, q, then computes their product N. She also computes $\varphi(N) = (p-1)(q-1)$. Then she takes an exponent $e \in \mathbf{N}$ coprime to $\varphi(N)$, and computes its inverse d modulo $\varphi(N)$. She publishes N, e and keeps $p, q, \varphi(N), d$ in secret.

Now anyone (say, Bob) can send her a message m (a residue class modulo N) using the following protocol. Bob raises the message to power e modulo N and sends $c \equiv m^e \bmod N$ to Alice.

Now Alice raises the incoming message c to power d modulo N. With high probability, m is coprime to N, and then, by Euler-Fermat,

$$c^d \equiv (m^e)^d \equiv m^{\varphi(N)u+1} \equiv (m^{\varphi(N)})^e \cdot m \equiv 1 \cdot m \equiv m \bmod N,$$

which is the original message.

(b) Assume $q = p + 2$. Then

$$N + 1 = pq + 1 = p(p+2) + 1 = p^2 + 2p + 1 = (p+1)^2,$$

that is,

$$p = \sqrt{N+1} - 1.$$

Therefore, Eve adds one to N, then takes the square-root. This square-root can be computed in polynomial time, as we learned it from a homework problem. Subtracting one from the square-root, we obtain p. Now clearly $q = N/p$ (again computed in polynomial time).

Having p, q in hand, Eve can do the same as Alice.

Namely, she can compute $\varphi(N)$, then d (the inverse of e modulo $\varphi(N)$) in polynomial time using the euclidean algorithm. Therefore, she can decrypt any cipher she intercepts by computing its dth power modulo N. (Of course, this works only for coprime-to-N plaintexts, but this is the case with high probability.)

2. (a) Describe the elliptic curve discrete logarithm problem. **(2 points)**

   (b) Let $\mathbf{R}$ be the base field. Prove that the affine elliptic curve

$$\{(x,y) \in \mathbf{R}^2 : y^2 = x^3 + Ax\}$$

   has exactly three intersection points with the x axis if and only if $A < 0$. **(4 points)**

Solution. (a) Let E be an elliptic curve. The elliptic curve discrete logarithm problem is, given $P, Q \in E$, to compute the smallest positive integer n satisfying that

$$Q = nP = \underbrace{P + \ldots + P}_{n \text{ times}}$$

holds.

(b) First assume that there are three such intersection points. Then $x^3 + Ax$ as a function from $\mathbf{R}$ to $\mathbf{R}$ cannot be a strictly monotone function, since it takes the value zero three times. If $A \geqslant 0$, then $x \mapsto x^3 + Ax$ is strictly monotone increasing, therefore $A < 0$ must hold.

For the converse, assume $A < 0$. Then observe that for $x = 0, \pm\sqrt{-A}$,

$$x^3 + Ax = x(x^2 + A) = 0,$$

so there are three intersection points: $(-\sqrt{-A}, 0), (0,0), (\sqrt{-A}, 0)$.

3. (a) Define entropy. **(2 points)**

   (b) Let $p_1, \ldots, p_n$ be positive real numbers such that $p_1 + \ldots + p_n = 1$. Let q and r be further positive real numbers such that $p_n = q + r$. Prove that

$$H(p_1, \ldots, p_n) < H(p_1, \ldots, p_{n-1}, q, r).$$

   (4 points)

Solution. (a) The entropy function H is defined on finite sets of positive numbers summing up to 1, i.e. on tuples $(p_1, \ldots, p_n) \in \mathbf{R}_+^n$ if $p_1 + \ldots + p_n = 1$, for any $n \in \mathbf{N}$. For such a tuple,

$$H(p_1, \ldots, p_n) = -\sum_{j=1}^{n} p_j \log_2 p_j.$$

(b) First of all, record that H is defined on $(p_1, \ldots, p_{n-1}, q, r)$, since

$$p_1 + \ldots + p_{n-1} + q + r = p_1 + \ldots + p_{n-1} + p_n = 1.$$

By the (H3) property of the entropy (which was stated for the decomposition of the first variable, but clearly H is symmetric in its variables), we have

$$H(p_1, \ldots, p_{n-1}, q, r) = H(p_1, \ldots, p_n) + p_n H(q, r).$$

Clearly $H(q, r) > 0$, which implies

$$H(p_1, \ldots, p_n) < H(p_1, \ldots, p_{n-1}, q, r),$$

and the proof is complete.

4. (a) State the Euler-Fermat theorem. **(2 points)**

   (b) Let $p > 2$ be a prime number such that $p \equiv 3 \bmod 4$. Assume a is a further integer, which is coprime to p. Assuming that a has a square-root modulo p, prove that $a^{(p+1)/4}$ is a square-root of a modulo p. **(4 points)**

Solution. (a) Assume $m \in \mathbf{N}$ and a is a further integer coprime to m. Then

$$a^{\varphi(m)} \equiv 1 \bmod m,$$

where $\varphi(m)$ is the number of modulo m residue classes coprime to m.

(b) Letting $b \equiv a^{(p+1)/4} \bmod p$, it suffices to see that its square is a modulo p. Denoting by c a square-root of a (which exists by assumption), we have

$$b^2 \equiv \left(a^{\frac{p+1}{4}}\right)^2 \equiv a^{\frac{p+1}{2}} \equiv a \cdot a^{\frac{p-1}{2}} \equiv a \cdot (c^2)^{\frac{p-1}{2}} \equiv a \cdot c^{p-1} \equiv a \bmod p,$$

in the last step, applying Euler-Fermat and $\varphi(p) = p - 1$.