THE UNIVERSITY OF SYDNEY
MATH3925 PUBLIC KEY CRYPTOGRAPHY

Semester 2 **Exercises and Solutions for Week 13** 2004

Exam Revision Questions

1. **a.** Find an isomorphism between $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ and $\mathbb{Z}/21\mathbb{Z}$.

b. What are the abelian invariants of $\mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/21\mathbb{Z}$?

Solution

a. We first define the map $\mathbb{Z}/21\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ by $1 \mapsto (1, 1)$, then use the Chinese Remainder Theorem to construct the inverse. A solution $3x + 7y = 1$ to the extended GCD provides congruences $7y \equiv 1 \bmod 3$ and $3x \equiv 1 \bmod 7$. Then the map $(a, b) \mapsto 7ya + 3xb$ satisfies

$$7ya + 3xb \equiv a \bmod 3,$$
$$7ya + 3xb \equiv b \bmod 7.$$

The particular solutions $x = -2$ and $y = 1$ let us write the inverse map as $(a, b) \mapsto 7a - 6b$.

b. The abelian invariants are $[7, 42]$, i.e. the group is isomorphic to the group $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/42\mathbb{Z}$.

2. **a.** Express the 2-torsion subgroup of $\mathbb{Z}/N\mathbb{Z}^*$ in terms of the factorization of N. Consider N odd, $N \equiv 2 \bmod 4$, $N \equiv 4 \bmod 8$ and $N \equiv 0 \bmod 8$.

b. Find the 2-torsion subgroup of $\mathbb{Z}/17{\cdot}19\mathbb{Z}^*$.

Solution

a. The 2-torsion of $\mathbb{Z}/N\mathbb{Z}^*$ is isomorphic to the product of the 2-torsion in $\mathbb{Z}/p^n\mathbb{Z}^*$, for each prime power $p^n || N$. For an odd prime p dividing N this contributes one copy of $\{\pm 1\}$. For $p = 2$, we have to consider the 2-torsion groups

$$\mathbb{Z}/2\mathbb{Z}^*[2] = \{1\},$$
$$\mathbb{Z}/4\mathbb{Z}^*[2] = \{\pm 1\},$$
$$\mathbb{Z}/8\mathbb{Z}^*[2] = \{\pm 1, \pm 5\}$$

The latter group is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and for any $n \geq 3$ the group $\mathbb{Z}/2^n\mathbb{Z}^*[2]$ is isomorphic. Explicitly the 2-torsion elements of this group are $\{\pm 1, \pm 1 + 2^{n-1}\}$.

b. The 2-torsion subgroup consists of those elements which reduce to ± 1 modulo 17 and 19. As in question 1(a), we find solutions $x = -10$ and $y = 9$ to $17x + 19y = 1$. Then the element $18 = 9 \cdot 19 + 10 \cdot 17$ is 1 modulo 17 and -1 modulo 19 so the four 2-torsion elements are $\{\pm 1, \pm 18\}$.

3. Let $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, let H be the subgroup generated by $(1, 2)$. Prove that each of the maps $\varphi : G \to \mathbb{Z}/4\mathbb{Z}$ given by (i) $\varphi(x, y) = 2x + y$, (ii) $\varphi(x, y) = 2x + 3y$, and (iii) $\varphi(x, y) = y$ are homomorphisms, and determine for which of the maps H is the kernel of φ.

Solution That each map is a homomorphism is clear since they are all linear. Since $(1, 2)$ is in the kernel of each of the first two maps, and not in the third, we conclude that $H = \ker(\varphi)$ for all but the last map.

4. **a.** Explain how relations $n^2 - m^2 \equiv 0 \bmod N$ determine factorizations of N. When does this give rise to a trivial factorization?

b. How do relations $n^2 - m^2 \equiv 0 \bmod N$ correspond to elements of the 2-torsion subgroup of $\mathbb{Z}/N\mathbb{Z}^*$?

c. Prove that any function that produces random elements of $\mathbb{Z}/N\mathbb{Z}^*[2]$ results in a probabilistic factorization algorithm for N.

d. Demonstrate this principle for $N = 851$, obtaining a factorization.

Solution

a. A relation $n^2 - m^2 \equiv 0 \bmod N$, for n and m coprime to N, yields a factorization $N = \mathrm{GCD}(N, n - m) \cdot \mathrm{GCD}(N, n + m)$. The trivial factorization results $n \equiv \pm m \bmod N$.

b. To any such n and m, the element $m^{-1}n$ is a 2-torsion of $\mathbb{Z}/N\mathbb{Z}^*$.

c. Any 2-torsion element u different from ± 1 yields a nontrivial factorization $N = \mathrm{GCD}(N, u - 1) \cdot \mathrm{GCD}(N, u + 1)$.

d. Note that $851 = 900 - 49 = 30^2 - 7^2$. Thus $\mathrm{GCD}(30 - 7, 851) - 23$ and $\mathrm{GCD}(30 + 7, 851) = 37$ are factors of 851; the associated 2-torsion elements are $\pm 30 \cdot 7^{-1}$.

5. Find the kernel of the homomorphism $\mathbb{Z}^4 \to \mathbb{Z}/37\mathbb{Z}^*$ taking the standard basis elements of $\mathbb{Z}^4$ to 2, 3, 5, and 7.

Solution We make use of the obvious relation $-1 = 2^2 3^2$ for reducing relations in which -1 occur. We observer the following elementary relations

$$
\begin{array}{lll}
1) & 2^4\,3^4 = 1 & (4,\ 4,\ 0,\ 0) \\
2) & 5 \cdot 7 = 37 - 2 = -2 = 2^3\,3^2 & (3,\ 2, -1, -1) \\
3) & 2 \cdot 3 \cdot 7 = 37 + 5 = 5 & (1,\ 1, -1,\ 1) \\
4) & 2 \cdot 3 \cdot 5 = 37 - 7 = -7 = 2^2\,3^2\,7 & (1,\ 1, -1,\ 1) \\
5) & 2^3\,5 = 40 = 3 & (3, -1,\ 1,\ 0)
\end{array}
$$

The relations 3) and 4) determine the same element of the kernel, but the remaining elements are independent and generate the kernel since the determinant of the basis matrix is $36 = \varphi(37)$.

6. **a.** Describe an algorithm to compute the Jacobi symbol

$$\left(\frac{a}{n}\right) \in \{\pm 1\},$$

and give an interpretation of this value when n is prime.

b. Define Euler, Fermat, and strong pseudoprimes.

c. Show that an Euler pseudoprime base a is a Fermat pseudoprime base a.

d. Describe the Miller–Rabin primality test.

Solution First we recall the algorithm defining of the Jacobi symbol – a group homomorphism from $\mathbb{Z}/n\mathbb{Z}^*$ to $\{\pm 1\}$, then the definitions of Fermat, Euler, and strong pseudoprime base a.

a. The Jacobi symbol is defined for n odd and $\mathrm{GCD}(a, n) = 1$. For two odd numbers a and n we define

$$\left(\frac{a}{n}\right) = (-1)^e \left(\frac{n}{a}\right)$$

where $e = (n-1)(a-1)/4$, and

$$\left(\frac{-1}{n}\right) = (-1)^{(n-1)/4} \qquad \left(\frac{2}{n}\right) = (-1)^{(n-1)/8}$$

and for prime n, the value of the Jacobi symbol is 1 when a is a square and -1 when a is a nonsquare. Since the Jacobi symbol is well-defined for any representative a mod n, we may recursively solve for the Jacobi symbol in terms of n mod a where we take a representative for n in the range $-a/2 < n \leq a/2$.

b. A *Fermat pseudoprime* n base a is an odd composite number which satisfies $a^{n-1} \equiv 1 \bmod n$.

An *Euler pseudoprime* n base a is an odd composite which satisfies

$$a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \bmod n,$$

where the right hand side is the *Jacobi symbol* of a mod n.

A *strong pseudoprime* base a is one which satisfies the condition that for a factorization $n - 1 = 2^t m$ with m odd, the sequence

$$a_0 = a^m \bmod n,\ a_1 = a_0^2 \bmod n,\ a_2 = a_1^2 \bmod n, \ldots$$

has a tail of 1's, and if $a_0 \neq 1$, then -1 preceeds the first occurrence of 1.

c. The test checks, for t randomly selected a in $\mathbb{Z}/N\mathbb{Z}^*$, whether N is a strong pseudoprime base a.

7. **a.** Describe the baby-step, giant-step algorithm, Pollard ρ algorithm, and index calculus algorithm for determining the factorization of an integer N.

b. Explain the applications of these algorithms, or modified versions of these algorithms, the discrete logarithm problem in $\mathbb{F}_p^*$.

Solution

a. Baby-step, giant-step: Given N be an integer and let g and h be in $\mathbb{Z}/N\mathbb{Z}^*$ such that h is in the cyclic subgroup generated by g. For the baby-step, giant-step algorithm, set s be the least integer greater than $\sqrt{N}$. Then form the indexed set of $1, g, g^2, \ldots, g^{s-1}$. Each element g^i should associated with its exponent i, and allow for efficient hashed lookup. Now compute h, then $hg^s, hg^{2s}, \ldots$ until finding a match $hg^{sj} = g^i$. Then the identity $h = g^{i-sj}$ holds, so $\log_g(h) = i - sj$.

Pollard ρ and index calculus: refer to the tutorial solutions and your lecture notes.

b. The goal of these algorithms in factorization is to find the group order n of $\mathbb{Z}/N\mathbb{Z}^*$. This is obtained by a relation of the form $x^i = x^j$, from which $n|(i-j)$. In computing a discrete logarithm $\log_x(y)$ the goal is to find a relation of the form $x^i y^k = x^j y^l$. Then, using the group order $p-1$, the discrete logarithm is $(i-j)(k-l)^{-1} \bmod (p-1)$, provided the inverse of $k-l$ exists.

8. Show that the knowledge of the order of $\mathbb{Z}/N\mathbb{Z}^*$ is probabilistically expected polynomial time equivalent to the factorization of N.

Solution If $\varphi(N)$ is given, we can partially factor it as $2^t m$, where m is odd. For random a we consider the sequence

$$a^m, a^{2m}, \ldots, a^{2^t m} = 1.$$

Since a^m is a random element element of $[m](Z/N\mathbb{Z})^*$, a group of order 2^t, it is equal to 1 with probability $1/2^t$. If not equal to 1, then some element of the sequence is a nontrivial 2-torsion element. With probability at most $1/(e-1)$, where $e = |\mathbb{Z}/N\mathbb{Z}^*[2]|$, that 2-torsion element is -1. In the worse-case senario ($t = 2, e = 4$) for any N, a random a determines a 2-torsion element u not equal to -1 with probability at least $1/2$. A nontrivial factorization ensues from $GCD(u^2-1, N) = GCD(u-1, N)GCD(u+1, N)$. Repeated application of random choice of a gives an expected polynomial time factorization.

9. How many subfields does $\mathbb{F}_{p^{36}}$ have?

Solution Nine: $\mathbb{F}_p$, $\mathbb{F}_{p^2}$, $\mathbb{F}_{p^3}$, $\mathbb{F}_{p^4}$, $\mathbb{F}_{p^6}$, $\mathbb{F}_{p^9}$, $\mathbb{F}_{p^{12}}$, $\mathbb{F}_{p^{18}}$, and $\mathbb{F}_{p^{36}}$.

10. Describe several classes of groups used in cryptography which are ammenable to index calculus attacks, and list the types of smoothness bases used for their construction.

Solution Both the RSA protocol, using a group $\mathbb{Z}/N\mathbb{Z}^*$ and ElGamal protocols in $\mathbb{F}_q^*$ are subject to index calculus attacks. The possible factorization bases are small primes in $\mathbb{Z}$ for $\mathbb{Z}/N\mathbb{Z}^*$ and unit groups of prime fields $\mathbb{F}_p^*$, small degree polynomials in $\mathbb{F}_p[x]$ for unit groups of large extensions $\mathbb{F}_q$ of a small prime field $\mathbb{F}_p$.

11. Suppose that $|E(\mathbb{F}_{11})| = 16$. What is the minimal polynomial of the Frobenius endomorphism π? What are the possible group structures for $E(\mathbb{F}_{11})$? What are the possible group structures for an arbitrary abelian group of order 16?

Solution Writing $16 = 11 + 4 + 1$, we find that the minimal polynomial of the Frobenius endomorphism is $X^2 + 4X + 11$. The possible groups of rational points on an elliptic curve of order 16 are

$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z},\ \text{or } \mathbb{Z}/16\mathbb{Z}.$$

Since the Weil pairing e_4 must take a pair of generators for the 4-torsion to a 4-th root of unity, we see that the first possibility is excluded over $\mathbb{F}_{11}$, since no 4-th root of unity exists in $\mathbb{F}_{11}^*$. This leaves only two possibilities for $E(\mathbb{F}_{11})$. An arbitrary abelian group of this order can be one of the above groups or

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},\ \text{or } \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$$

12. Let E be the elliptic curve $y^2 = x^3 + x + 3$ over $\mathbb{F}_{17}$. Given the points $P = (3, 13)$, and $Q = (7, 8)$ in $E(\mathbb{F}_{17})$, find $P + Q$.

Solution We solve for the line $L : y = ax + b$ passing through the points P and Q. The slope is $a = (13 - 8)/(3 - 7) = 5/(-4) = 3$ in $\mathbb{F}_{17}$, since $4 \cdot (-4) = -16 = 1$, and then we find $b = 4$. The third point of intersection of L with E is $R = (-1, 1)$. We obtain this point by making the substitution

$$y^2 = (3x + 4)^2 = x^3 + x + 3,$$

and solving the resulting equation $x^3 + 8x^2 + 11x + 4$ by dividing out $x - 3$ and $x - 7$. The value of y is obtained by substituting back into L. This means that $P + Q + R = O$, the group identity, so $-R = (-1, -1)$ is the sum $P + Q$.

13. Let E be the supersingular elliptic curve $y^2 = x^3 + 4x + 7$ over $\mathbb{F}_{13}$, $P = (7, 1) \in E(\mathbb{F}_{13})$ a point of order 7, and $Q = (5, 3)$ in $\langle P \rangle$.

- **a.** What are the group structures of $E(\mathbb{F}_{13})$ and $E(\mathbb{F}_{13^2})$?
- **b.** Let $\mathbb{F}_{13^2} = \mathbb{F}_{13}[x]/(x^2 - x + 2)$ and set $R = (0, 10\bar{x} + 8) \in E(\mathbb{F}_{13^2})[7]$. Given that $e_7(P, R) = \bar{x} + 3$ and $e_7(Q, R) = 4\bar{x} + 3$, find $\log_P(Q)$.

Solution

- **a.** One can check that the point $(6, 0)$ is a 2-torsion element, hence the group order of $E(\mathbb{F}_{13}$ is divisible by 14. But this is the only possibility for a group of size $13 - t + 1$ with $|t| \leq 2\sqrt{13}$. Therefore $t = 0$, E is supersingular, $E(\mathbb{F}_{13}) \cong \mathbb{Z}/14\mathbb{Z}$, and $E(\mathbb{F}_{13^2}) \cong (Z/14\mathbb{Z})^2$.
- **b.** One checks that both $\log_P(Q) = \log_{\bar{x}+3}(4\bar{x} + 3) = 4$.

14. Find the 2-torsion points on the elliptic curve E of the previous question. Which points are in $E(\mathbb{F}_{13})$ and which points are in $E(\mathbb{F}_{13^2})$?

Solution The 2-torsion points are the points of the form $(x_0, 0)$, since $-(x_0, 0) = (x_0, 0)$. We just need to find the roots x_0 of the polynomial $x^3 + 4x + 7$ over $\mathbb{F}_{13}$. Since $|E(\mathbb{F}_{13})| = 14$, there is only one 2-torsion point in $E(\mathbb{F}_{13})$, which corresponds to the root $x_0 = 6$. The other two nontrivial 2-torsion points come from the two roots x_0 of $x^2 + 6x + 1$ in $\mathbb{F}_{13^2}$.

15. Describe the ElGamal protocol as used on an elliptic curve. What data does a public key contain? What data does the private key contain?

Solution Refer to your lecture notes for the description of the protocol. The public key contains (E, P, Q, n, h) where E is an elliptic curve over a finite field $\mathbb{F}_q$, P is a point of order n, Q is an element of the group P generates, and h is the cofactor order $|E(\mathbb{F}_q)/\langle P\rangle|$. The private key is the discrete logarithm $x = \log_P(Q)$.

16. Compare the groups used in the RSA protocol and the ElGamal protocol.

Solution The group used for RSA is a unit group $\mathbb{Z}/N\mathbb{Z}^*$ for $N = p_1p_2$, where p_1 and p_2 are odd primes. This means that it is not cyclic, since the quotient groups $\mathbb{Z}/p_1\mathbb{Z}^*$ and $\mathbb{Z}/p_2\mathbb{Z}^*$ each have even group order. The group used for ElGamal is the cyclic group $\mathbb{F}_p^*$ of units in a finite field. Moreover by construction it must have a large prime order subgroup, which is often required to be $(p-1)/2$. In the case of the RSA groups, the largest possible order of a prime subgroup is $(p_1 - 1)/2$ or $(p_2 - 1)/2$, which are each on the order $\sqrt{N}$.

17. State the properties of the Weil pairing.

Solution The Weil pairing $e_n : E[n] \times E[n] \to \overline{\mathbb{F}}_q^*$ on an elliptic E over a finite field $\mathbb{F}_q$ is a map into the n-th roots of unity of $\overline{\mathbb{F}}_q^*$. If ζ_n is a generator for the n-th roots of unity, then the Weil pairing satisfies the following four properties:

a. *Bilinearity:*
$e_n(xP, yQ) = e_n(P, Q)^{xy}$ for all $P, Q \in E[n]$ and $x, y \in \mathbb{Z}$;

b. *Alternating:*
$e_n(Q, P) = e_n(P, Q)^{-1}$ for all P, Q in $E[n]$;

c. *Nondegeneracy:*
For every $P \in E[n]$ there exists $Q \in E[n]$ such that $e_n(P, Q) = \zeta_n$.

d. *Rationality:*
The Weil pairing induces a map

$$e_n : E(\mathbb{F}_{q^r})[n] \times E(\mathbb{F}_{q^r})[n] \to \mathbb{F}_{q^r}^*$$

for every finite extension $\mathbb{F}_{q^r}$ of $\mathbb{F}_q$.

18. Describe the MOV algorithm for reducing an elliptic curve discrete logarithm problem to a finite field discrete logarithm. Explain why this does not generally result in an efficient algorithm.

Solution See Tutorial 12 for discussion of the Weil pairing and MOV reduction. For general elliptic curves this method fails to be of practical use since the degree r of the extension $\mathbb{F}_{q^r}$ in which the image of the Weil pairing is defined (i.e. the field of definition for the full n-torsion subgroup $E[n]$) is exponential in $\log(q)$.

19. Give the definition of a supersingular elliptic curve in terms of the trace of the Frobenius endomorphism. Given a supersingular elliptic curve over $\mathbb{F}_p$, for a prime $p > 3$, prove that $E(\mathbb{F}_{p^2}) = E[p+1]$.

Solution Refer to the notes from class for the full proof. The basic idea is that $E(\mathbb{F}_{p^2}) = \ker(\pi^2 - 1)$, and, from the minimal polynomial of π, we see that $\pi^2 = -p-1$ so $E(\mathbb{F}_{p^2}) = E[p+1]$.

20. Let $E/\mathbb{F}_p$ with $|E(\mathbb{F}_p)| = p - t + 1$.

a. Determine the characteristic polynomial $\chi_r(x)$ of the r-th power π^r of the Frobenius endomorphism, for $1 \le r \le 4$.

b. Prove that the exponent of $E(\mathbb{F}_{p^r})$ divides $\chi_r(1)$ for all r.

c. Using the stronger result that $|E(\mathbb{F}_{p^r})| = \chi_r(1)$, find the order of $E(\mathbb{F}_{p^r})$ when $p = 7$, $t = 1$, and $1 \le r \le 5$.

Solution

a. Recall that the characteristic polynomial of π^r is equal to the characteristic polynomial of the r-th power of the matrix

$$F = \begin{pmatrix} 0 & 1 \\ -p & t \end{pmatrix},$$

and has the form $\chi_r(x) = x^2 - t_r x + p^r$, where t_r is its trace. The first few powers of this matrix are

$$F^2 = \begin{pmatrix} -p & t \\ -tp & t^2 - p \end{pmatrix} \text{ and } F^3 = \begin{pmatrix} -tp & t^2 - p \\ -t^2p + p^2 & t^3 - 2tp \end{pmatrix},$$

of trace $t_2 = t^2 - 2p$ and $t_3 = t^3 - 3tp$. Then $F^4 = (F^2)^2$ has trace $t_4 = t_2^2 - 2p^2 = t^4 - 4t^2p + 2p^2$.

b. We prove that the group exponent of $E(\mathbb{F}_{p^r})$ divides $\chi_r(1)$, by the observation that

$$O = (\pi^{2r} - t_r\pi^r + p^r)P = (1 - t_r + p^r)P = \chi_r(1)P$$

for every P in $E(\mathbb{F}_{p^r})$ since $\pi^r(P) = P$.

c. Substituting into the above formulas we get $t_2 = -13$, $t_3 = -20$, and $t_4 = 71$. Extending the calculations further for this value of t and p, we find $t_5 = 211$. We then find the numbers of points $p^r - t_r + 1$ to equal 7, 63, 364, 2331, and 16597.