The University of Sydney
Math3925 Public Key Cryptography

Semester 2 | **Exercises 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 $\mathbb{Z}/14\mathbb{Z} \times \mathbb{Z}/21\mathbb{Z}$?

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 $\mathbb{Z}/17{\cdot}19\mathbb{Z}^*$.

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.

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.

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.

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.

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 $\mathbb{F}_p^*$.

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.

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

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.

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?

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 $P + Q$.

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 $\log_P(Q)$.

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 $E(\mathbb{F}_{13^2})$?

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?

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

17. State the properties of the Weil pairing.

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.

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 $E(\mathbb{F}_{p^2}) = E[p + 1]$.

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 $1 \le r \le 5$.