Chapter 10

Square roots and factoring

10.1. Square roots modulo n

Exercise 10.1.1. Find all of the square roots of 49 mod $3^2 \cdot 5 \cdot 11$.

10.2. Cryptosystems

Exercise 10.2.1. One can also create a cryptosystem using binary addition. For example, our key could be the 20-letter word $k = 10111011101111011001$. Then we could encrypt by using bit-by-bit addition; that is, $0 \bigoplus 0 = 1 \bigoplus 1 = 0$ and $0 \bigoplus 1 = 1 \bigoplus 0 = 1$. Therefore if the plaintext is $p = 11100010101101000011$, then $c = p \bigoplus k$, namely

$$\begin{array}{rl} & \texttt{10111 01110 11110 11001} \\ \bigoplus & \texttt{11100 01010 11010 00011} \\ = & \texttt{01011 00100 00100 11010.} \end{array}$$

It is easy to recover the plaintext since $p = c \bigoplus k$. Prove that one can recover the key if one knows the ciphertext and the plaintext.

10.3. RSA

Exercise 10.3.1. Let $n = 11 \times 53$ be an RSA modulus with encryption exponent $e = 7$. Determine d, the decryption exponent, by hand, using the Euclidean algorithm and the Chinese Remainder Theorem.

Exercise 10.3.2. Let $n = 5891$ be an RSA modulus with encryption exponent $e = 29$ and decryption exponent $d = 197$. Use this information to factor n.

10.4. Certificates and the complexity classes $\mathtt{P}$ and $\mathtt{NP}$

Exercise 10.4.1. Assuming only that 2 is prime, provide a certificate that proves that 107 is prime.

Exercise 10.4.2. Let $F_m = 2^{2^m} + 1$ with $m \geq 2$ be a Fermat number.

(a) Prove that if there exists an integer q for which $q^{\frac{F_m - 1}{2}} \equiv -1 \pmod{F_m}$, then F_m is prime.
(b) Deduce an "if and only if" condition for the primality of F_m using exercise 8.5.4.

10.5. Polynomial time primality testing

Exercise 10.5.1. Let p^k be the highest power of prime p that divides n, with $k \geq 1$.

(a) Prove that p^k does not divide $\binom{n}{p}$.

(b) Deduce that n does not divide $\binom{n}{p}$.

(c) Show that if n is composite, then n does not divide all the coefficients of the polynomial $(1+x)^n - x^n - 1$.

Exercise 10.5.2. Use the previous exercise to show:

(a) n is prime if and only if $(x+1)^n \equiv x^n + 1 \pmod{n}$.

(b) If $(n, a) = 1$, then n is prime if and only if $(x+a)^n \equiv x^n + a \pmod{n}$.

(c) Prove that if n is prime, then $(x+a)^n \equiv x^n + a \pmod{(n, x^r - 1)}$ for any integer a with $(a, n) = 1$ and any $r > 1$.

10.6. Factoring methods

Exercise 10.6.1. Factor 1649 using Fermat's method.

Exercise 10.6.2. Show that $\prod_{i \in I} a_i$ is a square if and only if $\sum_{i \in I} v_i \equiv (0, 0, \ldots, 0) \pmod{2}$.

Additional exercises

Exercise 10.7.1. Suppose that n is odd with at least two distinct prime factors. Prove that for at least half of the pairs x, y with $0 \leq x, y < n$, $\gcd(x, n) = 1$ and $x^2 \equiv y^2 \pmod{n}$, we have $1 < \gcd(x - y, n) < n$.

Exercise 10.7.2. Factor $n = 62749$. Let $m = [\sqrt{n}] + 1 = 251$. Compute $(m+i)^2 \pmod{n}$ for $i = 0, 1, 2, \ldots$ and retain those residues whose prime factors are all ≤ 11. Therefore we have $251^2 \equiv 2^2 \cdot 3^2 \cdot 7$; $253^2 \equiv 2^2 \cdot 3^2 \cdot 5 \cdot 7$; $257^2 \equiv 2^2 \cdot 3 \cdot 5^2 \cdot 11$; $260^2 \equiv 3^2 7^2 \cdot 11$; $268^2 \equiv 3 \cdot 5^2 \cdot 11^2$; $271^2 \equiv 2^2 \cdot 3^5 \cdot 11 \pmod{n}$. Use this information to factor n.

Exercise 10.7.3. Alice is sending Bob messages using RSA with public key modulus $n = 2027651281$ and encryption exponent $e = 66308903$. Oscar recalls that n is the number Fermat factored in section 10.6. Find the decryption exponent for Oscar.

Exercise 10.7.4. Let n be prime and suppose $q_1, \ldots, q_k$ are the odd prime factors of $n - 1$.

(a) Prove that the product of these primes, $N_1 := q_1 \cdots q_k$, is $\leq n/2$.

(b)† To certify that $q_1, \ldots, q_k$ are prime we need the set of odd prime factors of $q_1 - 1, \ldots, q_k - 1$. Let's call those primes $p_1, \ldots, p_\ell$. Prove that the product of these primes, $N_2 := p_1 \cdots p_\ell$, is $\leq N_1/2^k$.

(c) Generalize this argument to show that if there are r primes to be certified at the jth stage, then $N_{j+1} \leq N_j/2^r$.

(d)† Prove that if there are m primes that were certified to be prime during all the steps of this argument, then $2^m \leq n$. Explain why this implies that primality testing is in `NP`.

Exercise 10.7.5.† Suppose n is an odd composite, and $a^{(n-1)/2} \equiv 1$ or $-1 \pmod{n}$ for every a with $(a, n) = 1$. Deduce that $a^{(n-1)/2} \equiv 1 \pmod{n}$ for every a with $(a, n) = 1$ and that n is a Carmichael number.

Appendix 10A. Pseudoprime tests using square roots of 1

10.8. The difficulty of finding all square roots of 1

Exercise 10.8.1. Find all bases b for which 15 is a base-b Euler pseudoprime.

Exercise 10.8.2.[†] We wish to show that every odd composite n is not a base-b Euler pseudoprime for some integer b, coprime to n. Suppose not, i.e., that n is a base-b Euler pseudoprime for every integer b with $(b, n) = 1$.

(a) Show that n is a Carmichael number.
(b) Show that if prime p divides n, then $p - 1$ cannot divide $\frac{n-1}{2}$.
(c) Deduce that $(b/n) \equiv (b/p) \pmod p$ for each prime p dividing n.
(d) Explain why (c) cannot hold for every integer b coprime to n.

Exercise 10.8.3. Prove that $F_n = 2^{2^n} + 1$ is either a prime or a base-2 strong pseudoprime.

Exercise 10.8.4. Prove that if n is a base-2 pseudoprime, then $2^n - 1$ is a base-2 strong pseudoprime and a base-2 Euler pseudoprime. Deduce that there are infinitely many base-2 strong pseudoprimes.

Exercise 10.8.5. Pépin showed that one can test Fermat numbers F_m for primality by using just one strong pseudoprime test; i.e., F_m is prime if and only if $3^{(F_m-1)/2} \equiv -1 \pmod{F_m}$.

(a) Use exercise 8.5.4 to show if F_m is prime, then $3^{(F_m-1)/2} \equiv -1 \pmod{F_m}$.
(b) In the other direction show that if $3^{(F_m-1)/2} \equiv -1 \pmod{F_m}$, then $\text{ord}_p(3) = 2^{2^m}$ whenever prime $p|F_m$.
(c) Deduce that $F_m - 1 \leq p - 1$ in (b) and so F_m is prime.

Exercise 10.8.6.[†] (a) Prove that $A := (4^p + 1)/5$ is composite for all primes $p > 3$.
(b) Deduce that A is a base-2 strong pseudoprime.

Exercise 10.8.7.[‡] How many witnesses are there mod n? Suppose that $n - 1 = 2^k m$ with m odd and $k \geq 1$, and that n has ω distinct prime factors. Let g_p be the largest odd integer dividing $(p - 1, n - 1)$, and let 2^{R+1} be the largest power of 2 dividing $\gcd(p - 1 : p|n)$.

(a) Prove that $R \leq k - 1$.
(b) Show that (10.8.1) is $1, 1, \ldots, 1$ if and only if $a^{g_p} \equiv 1 \pmod{p^e}$ for every prime power $p^e \| n$.
(c) Show that there are $\prod_{p|n} g_p$ such integers $a \pmod n$.
(d) Show that if (10.8.1) is $1, 1, \ldots, 1, -1, *, \ldots, *$, with r $*$'s at the end, then $0 \leq r \leq R$, and that this holds if and only if $a^{2^r g_p} \equiv -1 \pmod{p^e}$ for every prime power $p^e \| n$.
(e) Show that there are $\leq \prod_{p|n} 2^r g_p$ such integers $a \pmod n$.
(f) Show the number of strong pseudoprimes mod n is

$$\prod_{p|n}(2^R g_p) \cdot \left(1 + \frac{1}{2^\omega} + \frac{1}{2^{2\omega}} + \cdots + \frac{1}{2^{(R-1)\omega}} + \frac{2}{2^{R\omega}}\right).$$

(g) Prove that $2^R g_p \leq \frac{p-1}{2}$ and so deduce that the quantity in (f) is $\leq \frac{\phi(n)}{2^{\omega-1}}$, and so is $< \frac{1}{4}\phi(n)$ if $\omega \geq 3$.
(h) Show that there are $\leq \frac{1}{4}\phi(n)$ reduced residues mod n which are not witnesses, whenever $n \geq 10$ with equality holding if and only if either
- $n = pq$ where $p = 2m + 1, q = 4m + 1$ are primes with m odd, or
- $n = pqr$ is a Carmichael number with p, q, r primes each $\equiv 3 \pmod 4$ (e.g., $7 \cdot 19 \cdot 67$).

Appendix 10B. Factoring with squares

10.9. Factoring with polynomial values

Exercise 10.9.1. Show that if $r_i = r_j$, then $a_i a_j$ is a square times a y-smooth integer.

Exercise 10.9.2. Show that if ℓ, p, and q are primes $> y$ with $r_i = \ell p$, $r_j = pq$, and $r_k = \ell q$, then $a_i a_j a_k$ is a square times a y-smooth integer.

Appendix 10C. Identifying primes of a given size

10.10. The Proth-Pocklington-Lehmer primality test

Exercise 10.10.1 (Proth's Theorem)**.** Suppose that $n = k \cdot 2^m + 1$ where $k < 2^m$. Show that n is prime if and only if there exists an integer a for which $a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$.

Exercise 10.10.2. Suppose that $m > 1$.

(a) Show that $n = 2^m+1$ is prime if and only if $3^{2^{m-1}} \equiv -1 \pmod{n}$ if and only if $5^{2^{m-1}} \equiv -1 \pmod{n}$.

(b) Let $u_0 = 3$ and then $u_{m+1} = u_m^2$ for all $n \geq 0$. Prove that $2^m + 1$ is prime if and only if $u_{m-1} \equiv -1 \pmod{2^m + 1}$. (This should be easy to implement algorithmically.)

Appendix 10D. Carmichael numbers

10.11. Constructing Carmichael numbers

10.12. Erdős's construction

Appendix 10E. Cryptosystems based on discrete logarithms

10.13. The Diffie-Hellman key exchange

10.14. The El Gamal cryptosystem

Appendix 10F. Running times of algorithms

10.15. `P` and `NP`

10.16. Difficult problems

Appendix 10G. The AKS test

Exercise 10.17.1. Suppose that $(a, n) = 1$. Prove that n is prime if and only if $(x+a)^n \equiv x^n + a \pmod{n}$ in $\mathbb{Z}[x]$.

10.17. A computationally quicker characterization of the primes

10.18. A set of extraordinary congruences

Appendix 10H. Factoring algorithms for polynomials

10.19. Testing polynomials for irreducibility

Exercise 10.19.1. (a) Factor $x^4 + 1 \pmod 2$.

(b) If prime $p \equiv 1 \pmod 4$, show that we can factor $x^4 + 1$ as $(x^2 + b)(x^2 - b) \pmod p$ for some value of $b \pmod p$.

(c) If prime $p \equiv 3 \pmod 4$, show that we can factor x^4+1 as $(x^2+bx+a)(x^2-bx+a) \pmod p$, for some values of a and $b \pmod p$.

10.20. Testing whether a polynomial is squarefree

10.21. Factoring a squarefree polynomial modulo p

Exercise 10.21.1. (a) Suppose that $S_1, \ldots, S_m \subset \{1, \ldots, r\}$ with the property that for any $i \neq j$ there exists k such that $i \in S_k$ but $j \notin S_k$. Prove that for each h, $1 \leq h \leq r$, there is a subset $I_h \subset \{1, \ldots, m\}$ for which $\bigcap_{k \in I_h} S_k = \{h\}$.

(b) Let $P_1, \ldots, P_r$ be irreducible polynomials mod p. Suppose we are given a collection of polynomials $h_1(x), \ldots, h_m(x) \pmod p$ which are each products of some subset of the $P_i(x)$, with the property that for any $i \neq j$ there exists k such that P_i divides h_k but not P_j. Show that if we take all the possible gcds of the h_k, we will obtain each of the P_j.