Chapter 7

Power residues

7.1. Generating the multiplicative group of residues

Exercise 7.1.1. (a) Show that for *any integers* a and $m \geq 2$, there exist integers i and k, with $0 \leq i \leq m-1$ and $1 \leq k \leq m-i$ such that $a^{n+k} \equiv a^n \pmod{m}$ for every $n \geq i$.
(b) For each integer $m \geq 2$ determine an integer a such that $a \not\equiv 1 \pmod{m}$ but $a^2 \equiv a \pmod{m}$. (This explains why we need the hypothesis that $(a, m) = 1$ in Lemma 7.1.1.)

Exercise 7.1.2. Let $k := \mathrm{ord}_m(a)$ where $(a, m) = 1$.
(a) Show that $1, a, a^2, \ldots, a^{k-1}$ are distinct $\pmod{m}$.
(b) Deduce that $a^j \equiv a^i \pmod{m}$ if and only if $j \equiv i \pmod{k}$.

We see that $\mathrm{ord}_m(a)$ is the smallest period of the sequence $1, a, a^2, \ldots \pmod{m}$.

7.2. Fermat's Little Theorem

Exercise 7.2.1. Prove that our two versions of Fermat's Little Theorem are *equivalent* to each other (that is, easily imply one another).

Exercise 7.2.2. Prove that for any $m > 1$ if $(a, m) = 1$, then $\mathrm{ord}_m(a)$ divides $\phi(m)$ (by an analogous proof to that of Theorem 7.1).

Exercise 7.2.3. Prove Euler's Theorem using the idea in the "sets of reduced residues" proof of Fermat's Little Theorem, given above.

Exercise 7.2.4. Determine the last decimal digit of 3^{8643}.

7.3. Special primes and orders

Exercise 7.3.1. Show that if p is prime and q is a prime dividing $2^p - 1$, then $\mathrm{ord}_q(2) = p$.

Exercise 7.3.2.† Show that if prime p divides $F_n = 2^{2^n} + 1$, then $\mathrm{ord}_p(2) = 2^{n+1}$. Deduce that $p \equiv 1 \pmod{2^{n+1}}$.

7.4. Further observations

Exercise 7.4.1. (a) Show that if $n > 4$ is composite, then n divides $(n-1)!$.
(b) Show that $n \geq 2$ is prime if and only if n divides $(n-1)! + 1$.

Exercise 7.4.2. (a) Use the idea in Gauss's proof of Wilson's Theorem to show that

$$\prod_{\substack{1\le a\le n\\(a,n)=1}} a \equiv \prod_{\substack{1\le b\le n\\ b^2\equiv 1 \pmod n}} b \pmod n.$$

(b) Evaluate this product using exercise 3.8.3 or by pairing b with $n-b$.

Exercise 7.4.3. (a) Show that $\binom{p-1}{(p-1)/2} \equiv (-1)^{(p-1)/2} \pmod p$.

(b) Deduce that if $p \equiv 3 \pmod 4$, then $\left(\frac{p-1}{2}\right)! \equiv 1$ or $-1 \pmod p$.

(c) Deduce that if $p \equiv 1 \pmod 4$, then $\left(\frac{p-1}{2}\right)!$ is a root of $x^2 \equiv -1 \pmod p$.

7.5. The number of elements of a given order, and primitive roots

Exercise 7.5.1. Write each reduced residue mod p as a power of the primitive root a, and use this to evaluate $1^k + 2^k + \cdots + (p-1)^k \pmod p$ as a function of a and k. Use this to give another proof of Corollary 7.5.2.

Exercise 7.5.2. Let g be a primitive root modulo odd prime p.

(a) Prove that $g^a \equiv 1 \pmod p$ if and only if $p-1$ divides a.

(b) Show that $g^{(p-1)/2} \equiv -1 \pmod p$.

Exercise 7.5.3. Find all residues of order 5 mod 31, given that $2^5 \equiv 1 \pmod{31}$.

Exercise 7.5.4. (a) Prove that 2 is a primitive root (mod 13).

(b) *Use this* to determine all of the other primitive roots (mod 13).

Exercise 7.5.5. Let g be a primitive root modulo odd prime p.

(a) Prove that if m divides $p-1$, then g^m has order $\frac{p-1}{m}$.

(b)† Prove that $g^k \pmod p$ is a primitive root mod p if and only if $(k, p-1) = 1$.

(c) Deduce that there are $\phi(p-1)$ primitive roots mod p.

7.6. Testing for composites, pseudoprimes, and Carmichael numbers

Exercise 7.6.1. Show that squarefree n is a Carmichael number if and only if n is composite and divides $a^n - a$ for all integers a.

Exercise 7.6.2. Show that if n is a Carmichael number, then it is odd.

Exercise 7.6.3.† Show that if n is a Carmichael number, then it has at least three prime factors.

Exercise 7.6.4. Prove that if $6m+1$, $12m+1$, and $18m+1$ are all primes, then their product is a Carmichael number. (It is an open problem whether there exist infinitely many such prime triples, though it is not difficult to find examples, like $7 \times 13 \times 19$ and $37 \times 73 \times 109$.)

7.7. *Divisibility tests, again*

7.8. *The decimal expansion of fractions*

Exercise 7.8.1.† Suppose that p is an odd prime for which 10 is a primitive root. Let a_k be the least residue of $10^k \pmod p$, and suppose that $a_k/p = .\overline{r_k}$ where $1 \le r_k < 10^{p-1}$. Prove that r_k is obtained from r_1, by removing the leading k digits and concatenating them on to the end.

Exercise 7.8.2. Prove that the decimal expansion of every rational number is eventually periodic. (One can see why we need "eventually" with the example $\frac{1}{30} = .03333\ldots$.)

7.9. Primes in arithmetic progressions, revisited

Exercise 7.9.1. Generalize this argument to primes that are 1 (mod 4), to primes that are 1 (mod 5), and to primes that are 1 (mod 6).

Additional exercises

Exercise 7.10.1. Prove that we can write any polynomial $f(x)$ mod p of degree $\leq p-1$ as

$$f(x) \equiv \sum_{a=0}^{p-1} f(a)(1-(x-a)^{p-1}) \pmod{p}.$$

Exercise 7.10.2.† Prove that if $f(x) \in \mathbb{Z}[x]$ is monic and has degree d and if prime p divides $f(0), f(1), \dots, f(d)$, then $p \leq d$ and p divides $f(n)$ for all integers n.

Exercise 7.10.3. We will find all powers of 2 and 3 that differ by 1, a special case of Catalan's conjecture mentioned in section 6.4.

(a) What are the powers of 3 (mod 8)? What are the powers of 2 (mod 8)?
(b) Show that if $2^n - 3^m \equiv 1 \pmod 8$ for some positive integers m, n, then $n = 1$ or 2.
(c) Deduce that the only solutions to $2^n - 3^m = 1$ are $4 - 3 = 2 - 1 = 1$.
(d) Prove that if $3^m - 2^n = 1$ with m odd, then $m = n = 1$.
(e) Prove that if $3^{2k} - 2^n = 1$, then both $3^k - 1$ and $3^k + 1$ are powers of 2, and that this is only possible if $k = 1$. We deduce that the only solutions to $3^m - 2^n = 1$ are $3 - 2 = 9 - 8 = 1$.

(This is the proof of Levi ben Gershon from around 1320.)

Exercise 7.10.4.† Show that if $\binom{n}{3}$ with $n > 3$ has no more than one prime factor which is > 3, then $n = 3$, 4, 5, 6, 8, 9, 10, or 18. (Use exercise 7.10.3.)

Exercise 7.10.5. (a) Prove that if $a > 1$, then the order of a mod $N := a^q - 1$ is exactly q. Now let q be a prime.
(b) Deduce that if prime p divides $a^q - 1$ but not $a - 1$, then p is a prime $\equiv 1 \pmod q$.
(c) Prove that $(\frac{a^q-1}{a-1}, a-1) = (q, a-1)$.
(d)† Prove that there are infinitely many primes $\equiv 1 \pmod q$.

Exercise 7.10.6. Let p be an odd prime, and let x, y, and z be pairwise coprime, positive integers.

(a)† Prove that if p divides $z - y$, then $\frac{z^p-y^p}{z-y} \equiv p \pmod{p^2}$.
(b) Show that if $x^p + y^p = z^p$, then there exists an integer r for which $z - y = r^p$ or $z - y = p^{p-1}r^p$.

(This problem continues on from exercise 3.9.7.)

Exercise 7.10.7. Deduce Theorem 7.6 from (7.5.1) using the Möbius inversion formula (Theorem 4.4).

Exercise 7.10.8. Let p be a prime. Prove that every quadratic non-residue (mod p) is a primitive root if and only if p is a Fermat prime.

Exercise 7.10.9. Suppose that g is a primitive root modulo odd prime p. Prove that $-g$ is also a primitive root mod p if and only if $p \equiv 1 \pmod 4$.

Exercise 7.10.10. (a) Show that the number of primes up to N equals, exactly,

$$\sum_{2 \leq n \leq N} \frac{n}{n-1} \cdot \left\{ \frac{(n-1)!}{n} \right\} - \frac{2}{3}.$$

(Here $\{t\}$ is the fractional part of t, defined as in exercise 1.7.4(b).)
(b) Suppose that $n > 1$. Show that n and $n + 2$ are both odd primes if and only if $n(n + 2)$ divides $4((n - 1)! + 1) + n$.

Exercise 7.10.11. Prove that if $f(x) \in \mathbb{Z}[x]$ has degree $\leq p-2$, then $\sum_{a=0}^{p-1} f(a) \equiv 0 \pmod{p}$.

Exercise 7.10.12.† Let p be an odd prime and k be an odd integer which is $\not\equiv 1 \pmod{p-1}$. Prove that $1^k + 2^k + \cdots + (p-1)^k \equiv 0 \pmod{p^2}$.

Exercise 7.10.13.† Let $a_{n+1} = 2a_n + 1$ for all $n \geq 0$. Can we choose a_0 so that this sequence consists entirely of primes?

We define n to be a *base-b pseudoprime* if n is composite and $b^{n-1} \equiv 1 \pmod{n}$.

Exercise 7.10.14. Show that if n is not prime, then it a base-b pseudoprime if and only if $\mathrm{ord}_{p^k}(b)$ divides $n-1$ for every prime power p^k dividing n.

Exercise 7.10.15. Suppose that n is a squarefree, composite integer.
(a) Show that $\#\{a \pmod{p} : a^{n-1} \equiv 1 \pmod{p}\} = (p-1, n-1)$.
(b) Show that there are $\prod_{p|n}(p-1, n-1)$ reduced residue classes $b \pmod{n}$ for which n is a base-b pseudoprime.

Exercise 7.10.16. (a) Prove that if n is composite, then $\{b \pmod{n} : n \text{ is a base-}b \text{ pseudoprime}\}$ is a subgroup of the reduced residues mod n.
(b)† Prove that if n is not a Carmichael number, then it is not a base-b pseudoprime for at least half of the reduced residues $b \pmod{n}$.
(c)† Suppose that p and $2p-1$ are both prime and let $n = p(2p-1)$. Prove that $\#\{b \pmod{n} : n \text{ is a base-}b \text{ pseudoprime}\} = \frac{1}{2}\phi(n)$.

Exercise 7.10.17. (a) Show that if p is prime, then the Mersenne number $2^p - 1$ is either a prime or a base-2 pseudoprime.
(b) Show that every Fermat number $2^{2^n} + 1$ is either a prime or a base-2 pseudoprime.
(c) Show that p^2 divides $2^{p-1} - 1$ if and only if p^2 is a base-2 pseudoprime.

Exercise 7.10.18.† Prove that there are infinitely many base-2 pseudoprimes by proving and developing one of the following two observations:

- Start with 341, and show that if n is a base-2 pseudoprime, then so is $N := 2^n - 1$.
- Prove that if $p > 3$ is prime, then $(4^p - 1)/3$ is a base-2 pseudoprime.

Can you generalize either of these proofs to other bases?

Exercise 7.10.19. Let a, b, c be pairwise coprime positive integers. Prove that there exists a (unique) residue class $m_0 \pmod{abc}$ such that if $m \equiv m_0 \pmod{abc}$ and if $am+1$, $bm+1$, and $cm+1$ are all primes, then their product is a Carmichael number (for example, $a = 1, b = 2, c = 3$ in exercise 7.6.4 with $m_0 = 0$).

Exercise 7.10.20. Let D be a finite set of at least two distinct positive integers, the elements of which sum to n. Suppose that d divides n for every $d \in D$. Prove that if there exists an integer m for which $p_d := dnm + 1$ is prime for every $d \in D$, then $\prod_{d \in D} p_d$ is a Carmichael number. (In particular note the case in which n is perfect and D is the set of proper divisors of n. The perfect number 6, for example, gives rise to the triple $6m+1, 12m+1, 18m+1$, which we explored in exercise 7.6.4.)

Exercise 7.10.21. (a) Prove that .010010000100... is irrational. (Here we put a "1" two digits after the decimal point, then 3 digits later, then 5 digits later, etc., with all the other digits being 0, the spacings between the "1"'s being $p-1$ for each consecutive prime p.)
(b)† Develop this idea to find a large class of irrationals.

Appendix 7A. Card shuffling and Fermat's Little Theorem

7.11. Card shuffling and orders modulo n

Exercise 7.11.1.† An "in-shuffle" is the riffle shuffle that interlaces the cards the other way; that is, after one shuffle, the order becomes cards $27, 1, 28, 2, 29, \ldots, 52, 26$. Analyze this in an analogous way to the above, and determine how many "in-shuffles" it takes to get the cards back into their original order.

Exercise 7.11.2.† What happens when one performs riffle shuffles on n-card decks, with n even?

Exercise 7.11.3.‡ Suppose that the dealer alternates between in-shuffles and out-shuffles. How many such pairs of shuffles does it take to get the deck of cards back into their original order?

Exercise 7.11.4. Suppose that σ is a permutation on $\{1, \ldots, n\}$ and that $\sigma = C_1 \cdots C_k$ where $C_1, \ldots, C_k$ are disjoint cycles.

(a) Show that the order of σ equals the least common multiple of the lengths of the cycles C_j, $1 \le j \le k$.
(b) Use this to find the order of the permutation corresponding to an out-shuffle.
(c) Prove that if $n_1, \ldots, n_k$ are any set of positive integers for which $n_1 + \cdots + n_k = n$, then there exists a permutation $\sigma = C_1 \cdots C_k$ on $\{1, \ldots, n\}$, where each C_j has length n_j.
(d) Deduce that the maximum order, $m(n)$, of a permutation σ on $\{1, \ldots, n\}$ is given by

$$\max \operatorname{lcm}[n_1, \ldots, n_k] \text{ over all integers } n_1, \ldots, n_k \ge 1 \text{ for which } n_1 + \cdots + n_k = n.$$

Exercise 7.11.5.† Show that there is a permutation $\sigma = C_1 \cdots C_k$ on $\{1, \ldots, n\}$ of order $m(n)$ in which the length of each cycle is either 1 or a power of a distinct prime.

Exercise 7.11.6.† Use the previous exercise to determine $m(52)$.

Exercise 7.11.7.‡ Use exercise 5.4.3 to prove that $\log m(n) \sim \sqrt{n \log n}$.

7.12. The "necklace proof" of Fermat's Little Theorem

Exercise 7.12.1. Let p be prime. Let X denote a finite set and $f : X \to X$ where $f^p = i$, the identity map. (Here f^p means composing f with itself p times.) Let $X_{\text{fixed}} := \{x \in X : f(x) = x\}$.

(a) Prove that $|X| \equiv |X_{\text{fixed}}| \pmod p$.
Let G be a finite multiplicative group and $X = \{(x_1, \ldots, x_p) \in G^p : \ x_1 \cdots x_p = 1\}$.
(b)† Deduce that $\#\{g \in G : g \text{ has order } p\} \equiv |G|^{p-1} - 1 \pmod p$.
(c) Deduce that if p divides the order of finite group G, then G contains an element of order p. Combined with Lagrange's Theorem, Corollary 7.23.1 of appendix 7D, this is an "if and only if" criterion.

Exercise 7.12.2. Let p be a given prime.

(a) Use (4.12.3) of appendix 4C to determine the number of irreducible polynomials mod p of prime degree q.
(b) Deduce that $q^p \equiv q \pmod p$ for every prime q.
(c) Deduce Fermat's Little Theorem.

7.13. Taking powers efficiently

7.14. Running time: The desirability of polynomial time algorithms

Exercise 7.14.1. Justify that multiplying two residues mod m together and reducing mod m takes no more than $2d^2$ steps.

Exercise 7.14.2. Prove that the Euclidean algorithm works in polynomial time.

Appendix 7B. Orders and primitive roots

7.15. Constructing primitive roots modulo p

7.16. Indices / Discrete Logarithms

Exercise 7.16.1. (a) Show that $\mathrm{ind}_p(ab) \equiv \mathrm{ind}_p(a) + \mathrm{ind}_p(b) \pmod{p-1}$.
(b) Show that $\mathrm{ind}_p(1) = 0$ and $\mathrm{ind}_p(-1) = (p-1)/2$, irrespective of the base used.
(c) Show that $\mathrm{ind}_p(a^n) \equiv n\ \mathrm{ind}_p(a) \pmod{p-1}$.

Exercise 7.16.2. Suppose that g and h are two primitive roots mod p, where $h \equiv g^\ell \pmod{p}$.

(1) Show that $(\ell, p-1) = 1$.
(2) Show that the index with respect to g is ℓ times the index with respect to h, mod p.
(3) Prove that there exists an integer m for which $g \equiv h^m \pmod{p}$.

Exercise 7.16.3. (a) Suppose that k divides $p-1$. Show that a is a kth power mod p if and only if k divides $\mathrm{ind}_p(a)$.
(b) Show that if a has order m mod p, then $\{a^k \pmod{p} : 1 \le k \le m,\ (k,m) = 1\}$ is the set of residues mod p of order m.

7.17. Primitive roots modulo prime powers

Exercise 7.17.1. Use Euler's Theorem and Lemma 7.1.2 to prove that $\lambda(m)$ divides $\phi(m)$. Prove that there is a primitive root mod m if and only if $\lambda(m) = \phi(m)$.

Exercise 7.17.2.† Suppose that p^k is a prime power dividing n and let $m = \mathrm{ord}_p(2)$. Prove that $\mathrm{ord}_{p^k}(2)$ divides $n-1$ if and only if m divides $(p-1, n-1)$ and p^k divides $2^m - 1$.

Exercise 7.17.3. Let $x_n = a^n - b^n$ and suppose that $m = m_p$ is the smallest positive integer for which prime p divides x_m. In exercise 1.7.24 we proved that $p|x_n$ if and and only if $m|n$. Now suppose that $p^k \| x_m$, and $m|n$ so that $x_m|x_n$. Prove that the power of p that divides x_n/x_m equals the power of p that divides n/m. (This also follows from exercise 7.33.2(c).)

Exercise 7.17.4.† Suppose that $q^n - p^m = 1$ where p is prime, with $m \ge 1$ and $n \ge 2$.
(a) Prove that if $m = 1$, then $q = 2$, n is prime, and p is a Mersenne prime.
(b) Prove that $q - 1 = p^k$ for some integer $k \ge 0$.
For now assume that $k \ge 1$ (and use Lemma 7.17.1 throughout).
(c) Prove that n is a power of p.
(d) Prove that if $p^k > 2$, then $q^p - 1 = p^{k+1}$, which is impossible.
(e) Deduce that $p = 2$ and $q = 3$, so that $9 - 8 = 1$ by exercise 7.10.3.
Now we may assume that $m \ge 2$ and $k = 0$ so that $q = 2$.
(f) Suppose that r divides m with m/r odd. Prove that $p^r + 1 = 2^j$ for some integer $j \ge 1$.
(g) Deduce that $m = r$ and therefore that m is a power of 2.
(h) Deduce that $p^m + 1 \equiv 2 \pmod{8}$ so that $n = 1$, which is impossible.

Therefore the only solution to $q^n - p^m = 1$ with p prime and $m, n \ge 2$ is $3^2 - 2^3 = 1$.

Exercise 7.17.5.† Prove that $(1+x)^{p^r} \equiv (1+x^p)^{p^{r-1}} \pmod{p^r}$ for all prime powers p^r.

7.18. Orders modulo composites

Exercise 7.18.1.† Prove that $\lambda(m) < \phi(m)$ if m is divisible by $4p$ or pq for odd primes $p < q$.

Exercise 7.18.2. Determine $\lambda(65520)$.

Exercise 7.18.3. Prove that $a^{\lambda(m)} \equiv 1 \pmod{m}$ for all integers a coprime to m.

Exercise 7.18.4. Show that composite n is a Carmichael number if and only if $\lambda(n)$ divides $n-1$.

Exercise 7.18.5. Let $N_m(n) = \#\{x \pmod n : x^m \equiv 1 \pmod n\}$ for some given integer $m \geq 2$.
(a) Prove that $N_m(n)$ is a multiplicative function of n.
(b)† Prove that $x^m \equiv 1 \pmod n$ if and only if $x^g \equiv 1 \pmod n$ where $g = (m, \lambda(n))$.
(c) Deduce that $N_m(n) = N_g(n)$ where $g = (m, \lambda(n))$.
(d) Use Theorem 7.6 to determine $N_m(p)$ for every prime p.

Exercise 7.18.6. Prove that 2 is a primitive root mod 3^m for all $m \geq 1$, and mod 5^n for all $n \geq 1$, and mod 11^r for all $r \geq 1$.

Appendix 7C. Finding nth roots modulo prime powers

7.19. nth roots modulo p

Exercise 7.19.1. Show that the solutions $x \pmod m$ to $x^n \equiv a \pmod m$ are in 1-to-1 correspondence with the solutions $y \pmod m$ to $y^g \equiv a \pmod m$ where $g = (n, \lambda(m))$.

Exercise 7.19.2. Prove that if odd prime p does not divide a, then

$$\#\{x \pmod p : x^4 \equiv a \pmod p\} = \begin{cases} 0 \text{ or } 4 & \text{if } p \equiv 1 \pmod 4, \\ 0 \text{ or } 2 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

7.20. Lifting solutions

Exercise 7.20.1. Show that if prime $p \nmid an$, then the number of solutions $x \pmod{p^k}$ to $x^n \equiv a \pmod{p^k}$ does not depend on k.

7.21. Finding nth roots quickly

Exercise 7.21.1. Show that N is the largest divisor of $p-1$ with exactly the same prime factors as n.

Exercise 7.21.2. Determine the square roots of $3 \pmod{37}$ using the technique above.

Appendix 7D. Orders for finite groups

7.22. Cosets of general groups

Exercise 7.22.1. Show that every element of G belongs to a unique coset of H.

7.23. Lagrange and Wilson

Exercise 7.23.1. Prove that if a has order m in G, then $H := \{1, a, a^2, \dots, a^{m-1}\}$ is a subgroup of G.

Exercise 7.23.2. Let p be a prime which does not divide the order of the finite group G.
(a) Prove that G contains no elements of order p.
(b) Let $X = \{(x_1, \dots, x_p) \in G^p : x_1 \cdots x_p = 1\}$, and then use exercise 7.12.1(a) to prove that $|G|^{p-1} \equiv 1 \pmod p$.
(c) Deduce Fermat's Little Theorem by applying (b) to the cyclic groups of order a for $1 \leq a \leq p-1$.

7.24. Normal subgroups

Exercise 7.24.1. Prove that every finite cyclic group is isomorphic to some $\mathbb{Z}/n\mathbb{Z}$.

Exercise 7.24.2. Prove that if $|G|$ is a prime, then G is cyclic.

Exercise 7.24.3. Show that the product of the elements in a finite cyclic group G is 1 if $|G|$ is odd, and equals the (unique) element of G of order two if m is even.

Exercise 7.24.4. Prove that if G is a finite, simple, abelian group, then G is isomorphic to the additive, cyclic group $\mathbb{Z}/p\mathbb{Z}$, where p is a prime.

Exercise 7.24.5.† By taking $G = \mathbb{Z}/n\mathbb{Z}$ deduce the Fundamental Theorem of Arithmetic from the Jordan-Hölder Theorem.

Feit and Thompson showed that, otherwise, every non-cyclic finite simple group has even order.

Appendix 7E. Constructing finite fields

7.25. Classification of finite fields

Exercise 7.25.1. Let $\mathbb{F}$ be a finite field.

(a) Show that if prime q divides $|\mathbb{F}|$, then either $q \cdot 1 = 0$ or $|\mathbb{F}|/q \cdot 1 = 0$. Use an induction hypothesis to deduce that there exists a prime p such that $p \cdot 1 = 0$ in $\mathbb{F}$.

(b) Show that this prime p is unique.

(c) Begin with a non-zero element $a_1 \in \mathbb{F}$. If $a_2 \notin \{n_1a_1 : \ n_1 \in \mathbb{F}_p\}$, then show that $\{n_1a_1 + n_2a_2 : \ n_1, n_2 \in \mathbb{F}_p\}$ has p^2 distinct elements.

(d) Deduce by induction that there exist $a_1, \dots, a_r \in \mathbb{F}$ for some integer $r \geq 1$ such that

$$\mathbb{F} = \{n_1a_1 + n_2a_2 + \cdots + n_ra_r : \ n_1, \dots, n_r \in \mathbb{F}_p\},$$

the elements $n_1a_1 + n_2a_2 + \cdots + n_ra_r$ being all distinct, and so $\mathbb{F}$ has p^r elements.

Exercise 7.25.2. Verify that this indeed gives a field with p^r distinct elements.

Exercise 7.25.3. (a) Prove that if $d|p^r - 1$ for some integer $r \geq 1$, then there are precisely $\phi(d)$ elements in $\mathbb{F}_{p^r}$ of order d.

(b) Deduce that $\mathbb{F}_q^*$ is a cyclic group (and therefore has a generator/primitive root) for any prime power q.

Exercise 7.25.4. Show that the finite field of p^2 elements is not isomorphic to the integers mod p^2 (that is, $\mathbb{F}_{p^2} \ncong \mathbb{Z}/p^2\mathbb{Z}$).

Exercise 7.25.5. Fix prime p. Suppose that the sequence $(u_n)_{n\geq 1}$ of integers satisfies the linear recurrence $u_{n+d} \equiv a_{d-1}u_{n+d-1} + \cdots + a_0u_n \pmod p$, where d is minimal.

(a) Suppose that $u_{n+D} \equiv b_{D-1}u_{n+D-1} + \cdots + b_0u_n \pmod p$. Prove that either the $u_n \equiv 0 \pmod p$ for all n or $f(x) := x^d - a_{d-1}x^{d-1} - \cdots - a_1x - a_0$ divides $x^D - b_{D-1}x^{D-1} - \cdots - b_0$ mod p.

(b) Prove that if $f(x) \pmod p$ is irreducible and $u_j \not\equiv 0 \pmod p$ for some j, $0 \leq j \leq d-1$, then $(u_n)_{n\geq 1}$ is periodic mod p with period $p^d - 1$.

This implies that the upper bound in exercise 2.5.21 is best possible.

7.26. The product of linear forms in $\mathbb{F}_q$

Exercise 7.26.1.† Generalize this to the appropriate n-by-n determinant in $\mathbb{F}_q$, with proof.

Appendix 7F. Sophie Germain and Fermat's Last Theorem

7.27. Fermat's Last Theorem and Sophie Germain

Appendix 7G. Primes of the form $2^n + k$

7.28. Covering sets of congruences

Exercise 7.28.1. Deduce that $k \cdot 2^n + 1$ is composite for every integer $n \geq 0$ (with k as defined above).

Exercise 7.28.2. Prove that there exist infinitely many integers k for which $2^n + k$ is composite for every integer $n \geq 0$. (That is, there is no prime p equal to k plus a power of 2.)

Exercise 7.28.3. Let k be as above. Let x_n be a second-order linear recurrence sequence for which $x_n = 3x_{n-1} - 2x_{n-2}$ for all $n \geq 2$. Show that x_n is composite for all $n \geq 0$ if (a) $x_0 = k+1$ and $x_1 = k+2$ or (b) $x_0 = k+1$ and $x_1 = 2k+1$.

Exercise 7.28.4. Let ℓ be any positive integer for which $\ell \equiv -k \pmod{F_6 - 2}$. Prove that $\ell \cdot 2^n - 1$ and $|2^n - \ell|$ are composite for every integer $n \geq 0$. Deduce that a positive proportion of odd integers m cannot be written in the form $p + 2^n$ with p prime.

Exercise 7.28.5. Prove that $13 \cdot 20^k + 1$ is not prime for any $k \geq 1$.

Exercise 7.28.6.‡ Prove that if $n \geq 3$, then $F_n - 2 = F_0 F_1 \dots F_{n-1}$ cannot be written in the form $p + 2^k + 2^\ell$ where p is prime and $k > \ell \geq 0$.

7.29. Covering systems for the Fibonacci numbers

7.30. The theory of covering systems

Exercise 7.30.1. (a) Prove this.
(b)† Deduce that if $m_1 < m_2 < \dots < m_k$ in an exact covering system, then either $m_k = 1$ or $m_k = m_{k-1}$.

Appendix 7H. Further congruences

7.31. Fermat quotients

Exercise 7.31.1. (a) Show that $\binom{2p}{p} = 2\prod_{n=1}^{p-1}\left(1 + \frac{p}{n}\right)$.
(b) By expanding the product, deduce that for odd primes p, we have

$$\frac{1}{2}\binom{2p}{p} \equiv 1 + p\sum_{n=1}^{p-1}\frac{1}{n} + \frac{p^2}{2}\left(\left(\sum_{n=1}^{p-1}\frac{1}{n}\right)^2 - \sum_{n=1}^{p-1}\frac{1}{n^2}\right) \pmod{p^3}.$$

(c) Use Corollary 7.5.2 and exercise 7.10.12 to deduce that $\binom{2p}{p} \equiv 2 \pmod{p^3}$ for all primes $p > 3$.
(d)‡ Prove *Wolstenholme's Theorem* that, for any prime $p > 3$ and any integers $n \geq m \geq 0$,

$$\binom{np}{mp} \equiv \binom{n}{m} \pmod{p^3}.$$

(The difference is divisible by p^4 if and only if p divides the Bernoulli number B_{p-3}.)

Exercise 7.31.2. Prove that

$$\sum_{n=1}^{p-1} n^k q_p(n) \equiv \begin{cases} 1/2 \pmod p & \text{if } k=1, \\ B_{p-1+k} - B_k \pmod p & \text{if } 2 \le k \le p-1. \end{cases}$$

Exercise 7.31.3. Show that if $p > 3$, then $\prod_{j=1}^{p-1}(ap+j) \equiv (p-1)! \pmod{p^3}$ for every integer a.

Exercise 7.31.4. Prove that

$$\prod_{n=0}^{p-1}(x-n) - \prod_{n=0}^{p-1}(x+n) \equiv px^{p-1} \pmod{p^2}$$

in two ways. First deduce it from (7.31.8) and then prove it by substituting in $x = 0, 1, \dots, p-1$.

7.32. Frequency of p-divisibility

Appendix 7I. Primitive prime factors of recurrence sequences

7.33. Primitive prime factors

Exercise 7.33.1. (a) Use exercise 4.16.4 to prove that if $|a| \ge 2$, then $|\phi_n(a)| \ge \alpha\ |a|^{\phi(n)}$ where $\alpha = \alpha(a) := \prod_{k\ge1}(1 - 1/|a|^k)$. Note that $\alpha(a) \ge \alpha(2) = .288788\dots$.

(b)† Deduce that $a^n - 1$ has a primitive prime factor for every integer $a \ne -1, 0, 1$ and $n \ge 1$, except for the special cases $n = 1$, $a = 2$; or $n = 2$, $a = -1 \pm 2^k$ for some integer k; or $n = 3$, $a = -2$; or $n = 6$, $a = 2$.

Exercise 7.33.2.‡ Suppose that $(a, b) = 1$. Let Δ_m denote the discriminant of the minimum polynomial for $(X_k)_{k\ge0}$.

(a) Prove that y_m, z_m, and Δ_m are pairwise coprime.

(b) Show that $\Delta_m = \Delta^2 x_m^2$.

(c) Let m_d be the smallest positive integer for which $d|x_m$. Now let $m = m_p$ for some prime p, and suppose that $p^k \| x_m$, so that $m_p = m_{p^2} = \cdots = m_{p^k}$. Prove that $m_{p^{k+1}} = pm_p$ and, in general, $m_{p^{k+j}} = p^j m_p$ for all $j \ge 0$.

Exercise 7.33.3.† Suppose that $(a, b) = 1$ and that odd prime p divides Δ.

(a) Prove that $x_n \equiv n(a/2)^{n-1} \pmod\Delta$, and deduce that $m_p = p$.

(b) Show that if $p > 3$, then $x_n \equiv n(a/2)^{n-1} + \frac{n(n-1)(n-2)}{24} n^2\Delta(a/2)^{n-3} \pmod{\Delta^2}$ for all $n \ge 3$.

(c) Deduce that p divides x_p but p^2 does not.

7.34. Closed form identities and sums of powers

7.35. Primitive prime factors and second-order linear recurrence sequences

Exercise 7.35.1. Assume that if $n \ge n_0$, then x_n has a primitive prime factor which divides x_n to the power 1 (that is, p divides x_n but not p^2).

(a) Show that the equation $x_n = y^2$ has no solutions with $n \ge n_0$.

(b) Show that, for any integer $d \ge 1$, the equation $x_n = dy^2$ has at most one solution with $n \ge n_0$.

(c) Show that there are no finite sequences $n_0 \le n_1 < n_2 < \cdots < n_r$ such that $x_{n_1} x_{n_2} \dots x_{n_r}$ is a square.

(d) Make the same deductions assuming that if $n > n_0$, then x_n has a primitive prime factor which divides x_n to exactly an odd power.