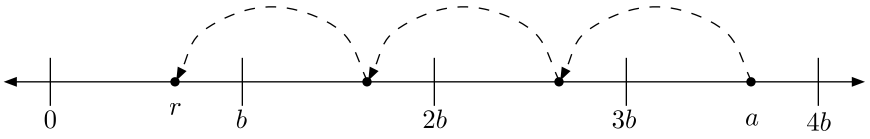
# Supplementary Material: *A Computational Introduction to Number Theory and Algebra (Version 1)*

Last updated: 10/15/2006.

This document contains supplementary exercises, examples, and a few alternative proofs of theorems that would make nice additions to the book, and may be added in a later edition.

## Section 1.1

After proof of Theorem 1.4, the following text might be helpful:

> Theorem 1.4 can be visualized as follows:
>
> 
>
>
> Starting with $a$, we subtract (or add, if $a$ is negative) the value $b$ until we end up with a number $r$ in the interval $\{0, \ldots, b-1\}$.

We can also add the following as an exercise in this section:

Exercise 1. Generalize Theorem 1.4 as follows. Let $a, b \in \mathbb{Z}$ with $b > 0$. Let $x, y$ be real numbers such that $y - x = b$. Show that there exist unique $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $r \in [x, y)$. Show the same, but for the interval $(y, x]$. Does the statement hold in general for the intervals $[x, y]$ or $(x, y)$?

## Section 1.2

Exercise 2. Let $a, n_1, \ldots, n_k$ be integers. Show that $\gcd(a, n_1 \cdots n_k) = 1$ if and only if $\gcd(a, n_i) = 1$ for $i = 1, \ldots, k$.

Exercise 3. For positive integer $m$, define $\mathcal{I}_m := \{0, \ldots, m-1\}$. Let $a, b$ be positive integers. Consider the map

$$\begin{aligned} \tau :\ & \mathcal{I}_b \times \mathcal{I}_a \to \mathcal{I}_{ab} \\ & (s, t) \mapsto (as + bt) \bmod ab. \end{aligned}$$

Show $\tau$ is a bijection if and only if $\gcd(a, b) = 1$.

## Section 2.1

EXERCISE 4. Let $w$ be a positive integer. For $a \in \{0, \ldots, 2^w - 1\}$, let $V(a)$ denote the integer obtained by inverting the bits in the $w$-bit, binary representation of $a$, so that $V(a) \in \{0, \ldots, 2^w - 1\}$. Show that $V(a) + 1 \equiv -a \pmod{2^w}$. This justifies the usual rule for computing negatives in 2's complement arithmetic (which is really just arithmetic modulo $2^w$).

After Exercise 2.5:

EXERCISE 5. Generalize Exercise 2.5 to odd prime powers. Specifically, show that if $p$ is an odd prime and $e$ is a positive integer, then $x^2 \equiv 1 \pmod{p^e}$ implies $x \equiv \pm 1 \pmod{p^e}$. Also show that the corresponding statement is false for $p = 2$. Hint: to prove the statement for odd $p$, show that if $(y + \epsilon)^2 \equiv 1 \pmod{p^e}$, where $p \mid y$ and $\epsilon = \pm 1$, then $p^e \mid y$.

## Section 2.2

Before Exercise 2.8:

EXERCISE 6. Let $n$ be a positive integer, let $a$ be any integer, and let $d := \gcd(a, n)$. Show that the number of integers $b \in \{0, \ldots, n - 1\}$ such that the congruence

$$az \equiv b \pmod{n}$$

has some integer solution $z$ is equal to $n/d$, and that for any such $b$, the number of integers $z \in \{0, \ldots, n - 1\}$ satisfying the congruence is equal to $d$.

EXERCISE 7. Let $p$ be an odd prime and $e$ a positive integer. Let $a$ and $b$ be integers not divisible by $p$. Show that $a^2 \equiv b^2 \pmod{p^e}$ if and only if $a \equiv \pm b \pmod{p^e}$. Hint: use Supplementary Exercise 5.

EXERCISE 8. For positive integer $m$, define $\mathcal{I}_m := \{0, \ldots, m-1\}$. Let $n_1, \ldots, n_k$ be positive, pairwise relatively prime integers and set $n := n_1 \cdots n_k$. Consider the map

$$\begin{aligned} \tau : \quad \mathcal{I}_n &\to \mathcal{I}_{n_1} \times \cdots \times \mathcal{I}_{n_k} \\ a &\mapsto (a \bmod n_1, \ldots, a \bmod n_k). \end{aligned}$$

Show that $\tau$ is a bijection. This is a simple consequence of the Chinese remainder theorem, and gives a perhaps more concrete way of thinking about that theorem (as illustrated was in Example 2.4).

EXERCISE 9. Let $f$ be a polynomial with integer coefficients. For positive integer $m$, define $Z_f(m)$ to be the set of integers $z \in \{0, \ldots, m - 1\}$ such that $f(z) \equiv 0 \pmod{m}$, and define $\omega_f(m) := |Z_f(m)|$. Show that the map $\tau$ defined in Supplementary Exercise 8 yields a one-to-one correspondence between $Z_f(n)$ and $Z_f(n_1) \times \cdots \times Z_f(n_k)$. Conclude that $\omega_f(n) = \omega_f(n_1) \cdots \omega_f(n_k)$.

EXERCISE 10. For a prime $p$, and integer $a$, let $\nu_p(a)$ denote the largest power of $p$ that divides $a$ (as was defined in §1.3). Let $p_1, \ldots, p_r$ be distinct primes, let $a_1, \ldots, a_r$ be arbitrary integers, and let $e_1, \ldots, e_r$ be arbitrary non-negative integers. Show that there exists an integer $x$ such that $\nu_{p_i}(x - a_i) = e_i$ for $i = 1, \ldots, r$.

## Section 2.3

EXERCISE 11. Let $n_1, \ldots, n_k$ be positive integers, and let $n := \prod_{i=1}^{k} n_i$. Consider the map

$$\begin{aligned} \rho : \quad \mathbb{Z}_n &\to \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k} \\ [a]_n &\mapsto ([a]_{n_1}, \ldots, [a]_{n_k}). \end{aligned}$$

(a) Show that the definition of $\rho$ is unambiguous, that is, $[a]_n = [a']_n$ implies $[a]_{n_i} = [a']_{n_i}$ for $i = 1, \ldots, k$.

(b) Show that if $\rho(\alpha) = (\alpha_1, \ldots, \alpha_k)$ and $\rho(\beta) = (\beta_1, \ldots, \beta_k)$, then $\rho(\alpha + \beta) = (\alpha_1 + \beta_1, \ldots, \alpha_k + \beta_k)$ and $\rho(\alpha\beta) = (\alpha_1\beta_1, \ldots, \alpha_k\beta_k)$.

(c) Using Supplementary Exercise 2, show that if $\rho(\alpha) = (\alpha_1, \ldots, \alpha_k)$, then $\alpha \in \mathbb{Z}_n^*$ if and only if $\alpha_i \in \mathbb{Z}_{n_i}^*$ for all $i = 1, \ldots, k$.

(d) Using the Chinese remainder theorem, show that if the $n_i$ are pairwise relatively prime, then $\rho$ is a bijection. Also show the converse: if $\rho$ is a bijection, then the $n_i$ must be relatively prime.

EXERCISE 12. Suppose $n$ is an odd, positive integer whose factorization into primes is $n = p_1^{e_1} \cdots p_r^{e_r}$. Consider the "squaring" map $\sigma : \mathbb{Z}_n^* \to \mathbb{Z}_n^*$ that sends $\alpha \in \mathbb{Z}_n^*$ to $\alpha^2 \in \mathbb{Z}_n^*$. Show that $\sigma$ is a $2^r$-to-1 map; that is, every square in $\mathbb{Z}_n^*$ has precisely $2^r$ distinct square roots. Hint: use Supplementary Exercises 7 and 11.

## Section 3.4

After Exercise 3.30:

EXERCISE 13. If the inputs $m_1, \ldots, m_r$ to the algorithm in the previous exercise are of greatly varying length, some improvements are possible.

(a) Suppose that the inputs satisfy $\operatorname{len}(m_i) \geq 2\operatorname{len}(m_{i-1})$ for $i = 2, \ldots, r$. Show how to modify your algorithm so that it uses $O(\operatorname{len}(m))$ multiplications in $\mathbb{Z}_n$.

(b) For general inputs, investigate how one can fine-tune the performance of your divide and conquer algorithm by optimizing the strategy used to split the given problem instance into subproblems, based on the relative lengths of the $m_i$. If you have some basic familiarity with information theory, show how to use Huffman codes to obtain an algorithm that uses $O(\operatorname{len}(m)(H(\ell_1/\ell, \ldots, \ell_r/\ell) + 1))$ multiplications in $\mathbb{Z}_n$, where $\ell_i := \operatorname{len}(m_i)$, $\ell := \sum_i \ell_i$, and $H(p_1, \ldots, p_r) := -\sum_i p_i \log_2 p_i$ is Shannon's entropy function. In addition to these multiplications, your algorithm may perform computations that take time $O(r \operatorname{len}(r))$ (which will be dominated by the time to perform the multiplications when $n$ is not too small).

## Section 3.5

Before Exercise 3.33:

Exercise 14. Let $M$ be a function mapping positive integers to positive reals. Show that $M$ is a well-behaved complexity function iff there exists a constant $c \geq 1$, such that for all positive integers $a$ and $b$, we have

$$1 \leq \frac{M(a+b)}{M(a)+M(b)} \leq c.$$

Also, show that the first inequality is implied by the condition that $N(\ell) := M(\ell)/\ell$ is a non-decreasing function.

## Section 4.1

Exercise 15. Let $a, b \in \mathbb{Z}$, with $a \geq b > 0$, let $d := \gcd(a, b)$, and let $q := a/d$. Show that Euclid's algorithm on inputs $a$ and $b$ runs in time $O(\operatorname{len}(b) \operatorname{len}(q))$.

## Section 4.5

Exercise 16. Let $n$ be a positive integer, and let $r^*, t^*$ be positive integers such that $r^* \leq n$ and $r^*t^* > n$. Show that for any integer $y$, there exist integers $r, t$ such that $ty \equiv \pm r \pmod{n}$, $0 \leq r < r^*$, and $0 < t < t^*$; moreover, show how to efficiently compute $r$ and $t$, given $n, r^*, t^*$, and $y$. Hint: adapt the proof of Theorem 4.6.

The following is a stronger version of Theorem 4.6. The proof is a bit more involved, but still reasonably short.

**Theorem 1.** *Let $r^*, t^*, n$ be positive integers with $n > 2r^*t^*$, and let $y$ be an integer with $0 \leq y < n$. Suppose that we run the extended Euclidean algorithm with inputs $a := n$ and $b := y$, and adopting the notation of Theorem 4.3, let $i$ be the smallest index among $1, \ldots, \ell + 1$ such that $r_i \leq r^*$, and define*

$$r' := r_i, \quad s' := s_i, \quad \textit{and} \quad t' := t_i.$$

*Moreover, suppose there exist integers $r, s, t$ such that*

$$r = sn + ty, \quad |r| \leq r^*, \quad \textit{and} \quad 0 < |t| \leq t^*. \tag{1}$$

*Then there exists a non-zero integer $\alpha$ such that*

$$r = r'\alpha, \quad s = s'\alpha, \quad \textit{and} \quad t = t'\alpha.$$

*Proof.* We begin with a simple observation. Since $r_0 > r_1 > \cdots > r_\ell > r_{\ell+1} = 0$, and $i$ is chosen to be the smallest index among $1, \ldots, \ell + 1$ such that $r_i \leq r^*$, we have

$$r_{i-1} > r^*. \tag{2}$$

The technical heart of the proof is to establish the following inequality:

$$|t_i| \leq t^*. \tag{3}$$

To prove (3), consider the following system of equations in the unknowns $\mu$ and $\nu$:

$$s_i\mu + s_{i-1}\nu = s, \tag{4}$$

$$t_i\mu + t_{i-1}\nu = t. \tag{5}$$

*Claim.* The system of equations (4), (5) has a unique solution $\mu, \nu$, and moreover, $\mu$ and $\nu$ are integers.

To prove the claim, we set $\epsilon := s_i t_{i-1} - s_{i-1}t_i = \pm 1$, and solve for $\mu$ and $\nu$ as follows. Subtracting $s_{i-1}$ times (5) from $t_{i-1}$ times (4) yields $\mu = (t_{i-1}s - s_{i-1}t)/\epsilon$. Similarly, subtracting $t_i$ times (4) from $s_i$ times (5) yields $\nu = (s_i t - t_i s)/\epsilon$. One can check that these values of $\mu$ and $\nu$ indeed satisfy (4) and (5), and are clearly integers. (Those familiar with linear algebra will see that the claim follows immediately from the fact that the matrix associated with the system of equations has determinant $\epsilon = \pm 1$, and so the above explicit calculations were not really necessary.)

We now use the claim to prove (3). We consider three cases.

(i) Suppose $\nu = 0$. In this case, (5) implies $t_i \mid t$, and since $t \neq 0$, this implies $|t_i| \leq |t| \leq t^*$.

(ii) Suppose $\mu\nu < 0$. In this case, since $t_i$ and $t_{i-1}$ have opposite sign, (5) implies $|t| = |t_i\mu| + |t_{i-1}\nu| \geq |t_i|$, and so again, we have $|t_i| \leq |t| \leq t^*$.

(iii) The only remaining possibility is that $\nu \neq 0$ and $\mu\nu \geq 0$. We argue that this is impossible. Adding $n$ times (4) to $y$ times (5), and using the identities $r_i = s_i n + t_i y$, $r_{i-1} = s_{i-1}n + t_{i-1}y$, and $r = sn + ty$, we obtain

$$r_i\mu + r_{i-1}\nu = r.$$

If $\nu \neq 0$ and $\mu$ and $\nu$ had the same sign, this would imply that $|r| = |r_i\mu| + |r_{i-1}\nu| \geq r_{i-1}$, and hence $r_{i-1} \leq |r| \leq r^*$; however, this contradicts (2).

That proves (3). The rest of the proof is much more straightforward. From the equalities $r_i = s_i n + t_i y$ and $r = sn + ty$, we have the two congruences:

$$r \equiv ty \pmod{n},$$

$$r_i \equiv t_i y \pmod{n}.$$

Subtracting $t_i$ times the first from $t$ times the second, we obtain

$$rt_i \equiv r_i t \pmod{n}.$$

This says that $n$ divides $rt_i - r_i t$. However, by hypothesis, we have

$$|r| \leq r^*, \quad |r_i| \leq r^*, \quad |t| \leq t^*, \quad \text{and} \quad 2r^*t^* < n,$$

and combined with the critical inequality (3), we obtain

$$|rt_i - r_i t| \leq |rt_i| + |r_i t| \leq 2r^*t^* < n.$$

Since $n$ divides $rt_i - r_it$ and $|rt_i - r_it| < n$, the only possibility is that

$$rt_i - r_it = 0. \tag{6}$$

Now consider the two equations:

$$\begin{aligned} r &= sn + ty, \\ r_i &= s_in + t_iy. \end{aligned}$$

Subtracting $t_i$ times the first from $t$ times the second, and using the identity (6), we obtain $n(st_i - s_it) = 0$, and hence

$$st_i - s_it = 0. \tag{7}$$

From (7), we see that $t_i \mid s_it$, and since $\gcd(s_i, t_i) = 1$, we must have $t_i \mid t$. So $t = t_i\alpha$ for some $\alpha$, and we must have $\alpha \neq 0$ since $t \neq 0$. Substituting $t_i\alpha$ for $t$ in equations (6) and (7) yields $r = r_i\alpha$ and $s = s_i\alpha$. □

## Section 5.1

**Theorem 5.2.** The following proof may be easier to follow:

> For positive integers $j, k$, define $d_{jk} := 1$ if $p^k \mid j$, and $d_{jk} := 0$, otherwise. Observe that $\nu_p(j) = \sum_{k\geq 1} d_{jk}$ (this sum is actually finite, since $d_{jk} = 0$ for all sufficiently large $k$). So we have
>
> $$\nu_p(n!) = \sum_{j=1}^{n} \nu_p(j) = \sum_{j=1}^{n}\sum_{k\geq 1} d_{jk} = \sum_{k\geq 1}\sum_{j=1}^{n} d_{jk}.$$
>
> Finally, note that $\sum_{j=1}^{n} d_{jk}$ is equal to the number of multiples of $p^k$ among the integers $1, \ldots, n$, which by Exercise 1.5 is equal to $\lfloor n/p^k \rfloor$.

## Section 6.1

Exercise 17. Let $\mathbf{D}_1 = (\mathcal{U}_1, \mathsf{P}_1), \mathbf{D}_2 = (\mathcal{U}_2, \mathsf{P}_2)$ be probability distributions, and let $\mathbf{D} = (\mathcal{U}_1 \times \mathcal{U}_2, \mathsf{P})$ be their product distribution.

(a) Show that if $\mathbf{D}_1$ is the uniform distribution on $\mathcal{U}_1$, and $\mathbf{D}_2$ is the uniform distribution on $\mathcal{U}_2$, then $\mathbf{D}$ is the uniform distribution on $\mathcal{U}_1 \times \mathcal{U}_2$.

(b) Show that if $\mathcal{A}_1 \subseteq \mathcal{U}_1$ and $\mathcal{A}_2 \subseteq \mathcal{U}_2$, then $\mathsf{P}[\mathcal{A}_1 \times \mathcal{A}_2] = \mathsf{P}_1[\mathcal{A}_1] \cdot \mathsf{P}_2[\mathcal{A}_2]$.

## Section 6.2

Exercise 18. Let $\mathbf{D}_1 = (\mathcal{U}_1, \mathsf{P}_1), \mathbf{D}_2 = (\mathcal{U}_2, \mathsf{P}_2)$ be probability distributions, and let $\mathbf{D} = (\mathcal{U}_1 \times \mathcal{U}_2, \mathsf{P})$ be their product distribution. Show that if $\mathcal{A}_1 \subseteq \mathcal{U}_1$ and $\mathcal{A}_2 \subseteq \mathcal{U}_2$, then with respect to $\mathbf{D}$, the events $\mathcal{A}_1 \times \mathcal{U}_2$ and $\mathcal{U}_1 \times \mathcal{A}_2$ are independent.

## Section 6.4

EXERCISE 19. Let $n \geq 1$, and consider a probabilistic experiment in which a subset $S \subseteq \{1, \ldots, n\}$ is chosen uniformly at random from the set of all $2^n$ subsets of $\{1, \ldots, n\}$. Define the random variable $X := |S|$. Show that $\mathsf{E}[X] = n/2$ and $\mathsf{E}[X^2] = (n^2 + n)/4$. Hint: write $X$ as a sum of indicator variables.

EXERCISE 20. Let $I$ be an interval of the real line (open, closed, or half open, bounded or unbounded), and let $f$ be a real-valued function defined on $I$. We say that $f$ is **convex on** $I$ if for all $x_0, x_2 \in I$, and for all $t \in [0, 1]$, we have $f(tx_0 + (1-t)x_2) \leq tf(x_0) + (1-t)f(x_2)$. Geometrically, convexity means that for any three points $P_i = (x_i, f(x_i))$, $i = 0, 1, 2$, where each $x_i \in I$ and $x_0 < x_1 < x_2$, the point $P_1$ lines on or below the line through $P_0$ and $P_2$. You may rely on the following analytical facts:

- if $f$ is convex on $I$, then $f$ is continuous on the interior of $I$ (but not necessarily at the endpoints of $I$, if any);
- if $f$ is continuous on $I$ and differentiable on the interior of $I$, then $f$ is convex on $I$ iff its derivative is non-decreasing on the interior of $I$.

(a) Prove **Jensen's inequality**: if $f$ is convex and $X$ is a random variable taking values in $I$, then $\mathsf{E}[f(X)] \geq f(\mathsf{E}[X])$. Hint: use induction on the size of the sample space.

(b) Using part (a), show that if $X$ takes non-negative real values, and $\alpha$ is a positive number, then $\mathsf{E}[X^\alpha] \geq \mathsf{E}[X]^\alpha$ if $\alpha \geq 1$, and $\mathsf{E}[X^\alpha] \leq \mathsf{E}[X]^\alpha$ if $\alpha \leq 1$.

(c) Using part (a), show that if $X$ takes positive real values, then

$$\mathsf{E}[X] \geq e^{\mathsf{E}[\log X]}.$$

(d) Using part (c), derive the **arithmetic/geometric mean inequality**: for positive numbers $x_1, \ldots, x_n$, we have

$$(x_1 + \cdots + x_n)/n \geq (x_1 \cdots x_n)^{1/n}.$$

## Section 6.6

We could add the following as a subsection at the end of this section:

### On the number of people with the same birthday

Related to the question of whether we expect any two people to have the same birthday is the following question:

> *how large do we expect the biggest subset of people with the same birthday to be?*

This is a bit harder to analyze, and we present only a partial analysis: we restrict ourselves to the setting where $n = k$ and $X_1, \ldots, X_n$ are mutually independent, with each uniformly distributed over $\{0, \ldots, n-1\}$; moreover, we only derive an asymptotic upper bound on the expectation (as $n$ tends to infinity).

We can formulate our problem more precisely as follows. For $x = 0, \ldots, n-1$, define the random variable $N_x$ to be the number of indices $i$ such that $X_i = x$; that is, $N_x$ represents the number of people whose birthday is $x$. We define

$$M := \max\{N_x : x = 0, \ldots, n-1\}.$$

Our goal is to estimate $\mathsf{E}[M]$.

Now, it is easy to see (verify) that for each $x$, we have $\mathsf{E}[N_x] = 1$; indeed, this holds even if the $X_i$ are not independent. However, even assuming the $X_i$ are mutually independent, estimating $\mathsf{E}[M]$ requires some work. We shall derive the following upper bound:

$$\mathsf{E}[M] \leq (\log n / \log\log n)(1 + o(1)). \tag{8}$$

In fact, it is known that

$$\mathsf{E}[M] \sim \log n / \log\log n,$$

and so our upper bound is in fact tight; however, we shall not derive this sharper result here.

To prove (8), we will use Theorem 6.8:

$$\mathsf{E}[M] = \sum_{m=1}^{n} \mathsf{P}[M \geq m]. \tag{9}$$

Let us upper bound the terms appearing in (9).

*Claim 1.* For $m = 1, \ldots, n$, we have $\mathsf{P}[M \geq m] \leq n/m!$.

Let $\mathcal{I}^{(m)}$ be the set of all subsets of $\{1, \ldots, n\}$ of size $m$. Now, $M \geq m$ if and only if there is an $x \in \{1, \ldots, n\}$ and a subset $\mathcal{J} \in \mathcal{I}^{(m)}$, such that $X_j = x$ for all $j \in \mathcal{J}$. We have

$$\begin{aligned}
\mathsf{P}[M \geq m] &\leq \sum_{x=1}^{n} \sum_{\mathcal{J} \in \mathcal{I}^{(m)}} \mathsf{P}\Big[\bigcap_{j \in \mathcal{J}} X_j = x\Big] \quad \text{(by (6.5))} \\
&= \sum_{x=1}^{n} \sum_{\mathcal{J} \in \mathcal{I}^{(m)}} \prod_{j \in \mathcal{J}} \mathsf{P}[X_j = x] \quad \text{(by mutual independence)} \\
&= n \binom{n}{m} n^{-m} \leq n/m!.
\end{aligned}$$

That proves Claim 1.

Of course, Claim 1 is only interesting when $n/m! \leq 1$, since $\mathsf{P}[M \geq m]$ always at most 1. Define $F(n)$ to be the smallest positive integer $m$ such that $m! \geq n$.

*Claim 2.* $F(n) \sim \log n / \log\log n$.

To prove this, let us set $m := F(n)$. It is clear that $n \leq m! \leq nm$, and taking logarithms, $\log n \leq \log m! \leq \log n + \log m$. Moreover, we have

$$\log m! = \sum_{\ell=1}^{m} \log \ell = \int_1^m \log t \, dt + O(\log m) = m \log m - m + O(\log m) \sim m \log m,$$

where we have estimated the sum by an integral (see §A2). Thus, $\log n = \log m! + O(\log m) \sim m \log m$. Taking logarithms again, we see that $\log\log n = \log m + \log\log m + o(1) \sim \log m$, and so $\log n \sim m \log m \sim m \log\log n$, from which Claim 2 follows.

Finally, observe that each term in the sequence $\{n/m!\}_{m=1}^{\infty}$ is at most half the previous term. Combining this observation with Claims 1 and 2, and the fact that $\mathsf{P}[M \geq m]$ is always at most 1, we have

$$\begin{aligned} \mathsf{E}[M] &= \sum_{m \geq 1} \mathsf{P}[M \geq m] = \sum_{m \leq F(n)} \mathsf{P}[M \geq m] + \sum_{m > F(n)} \mathsf{P}[M \geq m] \\ &\leq F(n) + \sum_{\ell \geq 1} 2^{-\ell} = F(n) + 1 \sim \log n / \log\log n. \end{aligned}$$

That proves (8).

That ends the additional subsection. After Exercise 6.26, we could add the following exercises, which generalize Exercises 6.25 and 6.26:

Exercise 21. Let $\alpha_1, \ldots, \alpha_n$ be non-negative numbers, with $\sum_{i=1}^{n} \alpha_i = 1$, and let $k$ be an integer between 2 and $n$. Define

$$P_k(\alpha_1, \ldots, \alpha_n) := \sum_{\{i_1, \ldots, i_k\}} \alpha_{i_1} \cdots \alpha_{i_k},$$

the sum being over all subsets of $k$ distinct indices between 1 and $n$. Show that $P_k(\alpha_1, \ldots, \alpha_n)$ is maximized when $\alpha_1 = \cdots = \alpha_n = 1/n$.

Exercise 22. Using the previous exercise, show the following. Suppose $X_1, \ldots, X_k$ are mutually independent random variables each uniformly distributed over a set $\mathcal{X}$ of size $n$. Let $\alpha$ be the probability that the $X_i$ values are distinct. Suppose $Y_1, \ldots, Y_k$ are mutually independent random variables, each taking values in $\mathcal{X}$, and each with the same distribution (not necessarily uniform). Let $\beta$ be the probability that the $Y_i$ values are distinct. Show that $\beta \leq \alpha$. This says that if the distribution of birthdays is skewed away from uniform (as it is for real people), we are more likely to see two people with the same birthday.

Yet another exercise:

Exercise 23. Suppose $k$ people have birthdays uniformly and independently distributed over an $n$-day year. Let $\mathcal{A}$ be the event that there is some day on which no birthdays fall. Show that if $k \geq n(\log n + t)$ for $t \geq 0$, then $\mathsf{P}[\mathcal{A}] \leq e^{-t}$.

## Section 6.7

Exercise 24. For positive integer $m$, define $\mathcal{I}_m := \{0, \ldots, m-1\}$. Let $n$ be a power of 2, let $\mathcal{A} := \mathcal{I}_n^{\times t}$ and $\mathcal{Z} := \mathcal{I}_n$. Define the family of hash functions $\mathcal{H}$ from $\mathcal{A}$ to $\mathcal{Z}$ as follows:

$$\mathcal{H} := \{h_{x_1, \ldots, x_t, y} : x_1, \ldots, x_t, y \in \mathcal{I}_{n^2}\},$$

where

$$h_{x_1, \ldots, x_t, y}(a_1, \ldots, a_t) := \lfloor ((a_1 x_1 + \cdots + a_n x_n + y) \bmod n^2)/n \rfloor.$$

Show that $\mathcal{H}$ is pairwise independent.

## Section 6.7.1

After Exercise 6.34:

EXERCISE 25. This exercise shows that the upper bound of Exercise 6.34 cannot be improved, without assuming something stronger than pairwise independence. Let $\ell$ be a positive integer, let $n := \ell^2 - \ell + 1$, and $\mathcal{Z} := \{0, \ldots, n-1\}$. Also let $\mathcal{S}$ be the set of all subsets of $\mathcal{Z}$ of size $\ell$, and let $\mathcal{F}$ be the set of all permutations on $\mathcal{Z}$. For $V \in \mathcal{S}$, let $\psi_V$ be some function that maps $V$ onto 0, and maps $\mathcal{Z} \setminus V$ injectively into $\mathcal{Z} \setminus \{0\}$. For $f \in \mathcal{F}$, $V \in \mathcal{S}$, and $a \in \mathcal{Z}$, define $\phi_{f,V}(a) := f(\psi_V(a))$. Finally, define $\mathcal{H} := \{\phi_{f,V} : f \in \mathcal{F}, V \in \mathcal{S}\}$. Show that $\mathcal{H}$ is a pairwise independent family of hash functions from $\mathcal{Z}$ to $\mathcal{Z}$, yet under any hash function in $\mathcal{H}$, there are at least $n^{1/2}$ elements of $\mathcal{Z}$ that hash to the same value.

After Exercise 6.35:

EXERCISE 26. Let $\mathcal{H}$ be an $\epsilon$-universal family of hash functions from $\mathcal{A}$ to $\mathcal{Y}$ (see Exercise 6.35), and let $\mathcal{H}'$ be an $\epsilon'$-universal family of hash functions from $\mathcal{Y}$ to $\mathcal{Z}$. Define the composed family $\mathcal{H}' \circ \mathcal{H}$ of hash functions from $\mathcal{A}$ to $\mathcal{Z}$ as $\mathcal{H}' \circ \mathcal{H} := \{\phi_{h',h} : h' \in \mathcal{H}', h \in \mathcal{H}\}$, where $\phi_{h',h}(a) := h'(h(a))$ for $\phi_{h',h} \in \mathcal{H}' \circ \mathcal{H}$ and $a \in \mathcal{A}$. Show that $\mathcal{H}' \circ \mathcal{H}$ is $(\epsilon + \epsilon')$-universal.

EXERCISE 27. Let $n$ be a prime.

(a) For positive integer $t$, let $\mathcal{H}_t := \{h_x : x \in \mathbb{Z}_n\}$ be the family of hash functions from $\mathbb{Z}_n^{\times(2t)}$ to $\mathbb{Z}_n^{\times t}$, defined as follows:

$$h_x(a_1, b_1, \ldots, a_t, b_t) := (a_1 + b_1 x, \ldots, a_t + b_t x).$$

Show that $\mathcal{H}_t$ is $1/n$-universal.

(b) Generalize part (a) as follows. Let $\mathcal{H}$ be a family of hash functions from $\mathcal{A}$ to $\mathcal{Z}$. For positive integer $t$, define the family $\mathcal{H}^{(t)} := \{\phi_h : h \in \mathcal{H}\}$ of hash functions from $\mathcal{A}^{\times t}$ to $\mathcal{Z}^{\times t}$ as follows:

$$\phi_h(a_1, \ldots, a_t) := (h(a_1), \ldots, h(a_t)).$$

Show that if $\mathcal{H}$ is $\epsilon$-universal, then $\mathcal{H}^{(t)}$ is $\epsilon$-universal.

(c) Now combine part (a) with Supplemental Exercise 26 to obtain, for every positive integer $s$, an $s/n$-universal family $\mathcal{H}'_s$ of hash functions from $\mathbb{Z}_n^{\times 2^s}$ to $\mathbb{Z}_n$, so that $\mathcal{H}'_s$ is in one-to-one correspondence with $\mathbb{Z}_n^{\times s}$.

The above exercise illustrates how one can use hash functions whose descriptions are much shorter that their input lengths, if one is willing to accept a somewhat higher collision probability. Later exercises will develop better trade-offs between description size and collision probability.

## Section 6.7.2

Add to Exercise 6.36:

Also show that $\mathcal{H}$ is $\epsilon$-universal (see Exercise 6.35).

## Section 6.8

EXERCISE 28. Let $X$ and $Y$ be random variables taking values in $[0, M]$. Let $\epsilon := \Delta[X; Y]$. Show that $|\mathsf{E}[X] - \mathsf{E}[Y]| \leq M\epsilon$.

## Section 6.9

EXERCISE 29. Suppose that in Theorem 6.21, $\mathcal{H}$ is a $(1 + \epsilon)/n$-universal family of hash functions (see Exercise 6.35). Show that the conclusion of the theorem holds with $\delta \leq \sqrt{n\kappa + \epsilon}/2$.

EXERCISE 30. Let $\mathcal{H}$ be a family of hash functions from $\mathcal{A}$ to $\mathcal{Z}$, and let $H$ denote a random variable uniformly distributed over $\mathcal{H}$. We say $\mathcal{H}$ is pairwise $\epsilon$-independent if for all $a \in \mathcal{A}$, the distribution of $H(a)$ is the uniform distribution over $\mathcal{Z}$, and for all $a' \in \mathcal{A} \setminus \{a\}$ and all $z \in \mathcal{Z}$, the conditional distribution of $H(a')$ given that $H(a) = z$ is $\delta$-uniform on $\mathcal{Z}$ for some $\delta \leq \epsilon$.

(a) Suppose $\mathcal{H}$ is a pairwise $\epsilon$-independent family of hash functions from $\mathcal{A}$ to $\mathcal{Z}$. Show that $\mathcal{H}$ is pairwise $(1/|\mathcal{Z}| + \epsilon)$-predictable (see Exercise 6.38).

(b) Now let $\mathcal{H}$ be an $\epsilon$-universal family of hash functions from $\mathcal{A}$ to $\mathcal{Y}$ (see Exercise 6.35), and let $\mathcal{H}'$ be a pairwise $\epsilon'$-independent family of hash functions from $\mathcal{Y}$ to $\mathcal{Z}$. Show that the family of hash functions $\mathcal{H}' \circ \mathcal{H}$ (see Exercise 6.40) is pairwise $(\epsilon + \epsilon')$-independent.

## Section 6.10

EXERCISE 31. This exercise extends Jensen's inequality (see Supplementary Exercise 20) to the discrete setting. Suppose that $f$ is a convex function on an interval $I$. Let $X$ be a random variable defined on a discrete probability distribution, taking values in $I$, and assume that both $\mathsf{E}[X]$ and $\mathsf{E}[f(X)]$ exist. Show that $\mathsf{E}[f(X)] \geq f(\mathsf{E}[X])$. Hint: use continuity.

## Section 7.1

EXERCISE 32. Let $\Lambda$ be a countable set, and let $\ell$ be a function mapping elements of $\Lambda$ to non-negative integers. Suppose that $\sum_{\lambda \in \Lambda} 2^{-\ell(\lambda)} \leq 1$. Show that there exists an injective function $\sigma$ mapping elements of $\Lambda$ to bit strings, such that $|\sigma(\lambda)| = \ell(\lambda)$ for all $\lambda \in \Lambda$, and the set $\{\sigma(\lambda) : \lambda \in \Lambda\}$ is prefix free.

## Section 7.4

After Exercise 7.13:

EXERCISE 33. You are to design and analyze an efficient probabilistic algorithm $B$ that takes as input two integers $n$ and $a$, with $n > 0$ and $0 \leq a \leq n$, and always outputs 0 or 1. Your algorithm should satisfy the following property. If $N$ is any deterministic algorithm that on input $x$ always outputs a positive integer, and is $A$ any probabilistic algorithm that on input $x$ always outputs an integer between 0 and $N(x)$, then $\mathsf{P}[B(N(x), A(x)) = 1] = \mathsf{E}[A(x)]/N(x)$.

## Section 7.5

EXERCISE 34. Consider the following recursive, probabilistic algorithm $A$, which takes as input a finite set $S$ of items, and returns a triple of integers $(d, \ell, q)$:

```
Algorithm $A(S)$:
    if $|S| \leq 1$ then
        $(d, \ell, q) \leftarrow (0, 0, 0)$
    else
        choose $S_1 \subseteq S$ at random (so every subset of $S$ is equally likely)
        $S_2 \leftarrow S \setminus S_1$
        $(d_1, \ell_1, q_1) \leftarrow A(S_1)$, $(d_2, \ell_2, q_2) \leftarrow A(S_2)$
        $(d, \ell, q) \leftarrow (\max\{d_1, d_2\} + 1, \ell_1 + \ell_2 + |S|, q_1 + q_2 + |S|^2)$
    return $(d, \ell, q)$
```

Let $(D, L, Q)$ denote the output of $A$ on input $S$, and let $n := |S|$. Show that $\mathsf{E}[D] = O(\log n)$, $\mathsf{E}[L] = O(n \log n)$, and $\mathsf{E}[Q] = O(n^2)$. Hint: Supplementary Exercise 19 may be useful.

## Section 8.1

EXERCISE 35. For a finite abelian group, one can completely specify the group by writing down the group operation table. For instance, Example 2.5 presented an addition table for $\mathbb{Z}_6$.

(a) Write down group operation tables for the following finite abelian groups: $\mathbb{Z}_5$, $\mathbb{Z}_5^*$, and $\mathbb{Z}_3 \times \mathbb{Z}_3$,.

(b) Below is an addition table for an abelian group that consists of the elements $\{a, b, c, d\}$; however, some entries are missing. Fill in the missing entries, and argue that there is only one way to do so.

| $+$ | $a$ | $b$ | $c$ | $d$ |
|---|---|---|---|---|
| $a$ | $a$ | | | |
| $b$ | $b$ | $a$ | | |
| $c$ | | | $a$ | |
| $d$ | | | | |

EXERCISE 36. Let $S$ be an arbitrary, non-empty set, and let $G$ be an abelian group. Let $\mathrm{Map}(S, G)$ be the set of all functions $f : S \to G$. For $f_1, f_2 \in \mathrm{Map}(S, G)$, define $f_1 + f_2 \in \mathrm{Map}(S, G)$ to be the function that maps $s \in S$ to $f_1(s) + f_2(s) \in G$. Show that $\mathrm{Map}(S, G)$ is an abelian group.

EXERCISE 37. Let $G$ be the set of all infinite bit strings; that is,

$$G = \{a_0 a_1 a_2 \cdots : a_i \in \{0, 1\}\}.$$

Define addition of elements of $G$ as follows. If $a = a_0a_1a_2\cdots$ and $b = b_0b_1b_2\cdots$, then $a + b = c = c_0c_1c_2\cdots$, where the $c_i$ are defined by the following formulas:

$$\mathit{carry}_0 = 0$$

and for $i = 0, 1, 2, \ldots$,

$$t_i = a_i + b_i + \mathit{carry}_i,\ c_i = t_i \bmod 2, \mathit{carry}_{i+1} = \lfloor t_i/2 \rfloor \in \{0, 1\}.$$

Show that $G$ is an abelian group. Intuitively, an element $a_0a_1a_2\cdots$ of $G$ acts like an "infinite binary number" $(\cdots a_2a_1a_0)_2$, with $a_0$ being the "low order bit."

## Section 8.2

Exercise 38. Let $G$ be an abelian group, and $H$ a non-empty subset of $G$ such that (i) $h \in H$ implies $-h \in H$, and (ii) $h \in H$ and $g \in G \setminus H$ implies $h + g \in G \setminus H$. Show that $H$ is a subgroup of $G$.

Exercise 39. Let $\mathrm{Map}(S, G)$ be defined as in Supplementary Exercise 36. Let $\mathrm{Map}'(S, G)$ be the set of elements $f$ of $\mathrm{Map}(S, G)$ such that $f(s) \neq 0$ for at most finitely many $s \in S$. Show that $\mathrm{Map}'(S, G)$ is a subgroup of $\mathrm{Map}(S, G)$.

## Section 8.4

The following exercise may replace Exercises 8.17 and 8.18:

Exercise 40. Let $G$ be an abelian group, and $n$ a positive integer. Show that $G^{\times n}$ and $\mathrm{Map}(\{1, \ldots, n\}, G)$ are isomorphic (see Supplementary Exercise 36).

Exercise 41. Let $G$ and $G'$ be abelian groups, and consider the abelian group $\mathrm{Map}(G, G')$ (see Supplementary Exercise 36). Let $\mathrm{Hom}(G, G')$ be the subset of elements of $\mathrm{Map}(G, G')$ that are group homomorphisms from $G$ into $G'$. Show that $\mathrm{Hom}(G, G')$ is a subgroup of $\mathrm{Map}(G, G')$.

## Section 8.5

Exercise 42. Let $G := \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$, where $m_1 \mid m_2$.

(a) Suppose $a \in G$ has order $m_2$. Show that $G/\langle a \rangle \cong \mathbb{Z}_{m_1}$.

(b) Suppose $a$ and $b$ are chosen at random from $G$. Show that $\langle a, b \rangle = G$ with probability at least $\phi(m_1)\phi(m_2)/m_1m_2$.

Exercise 43. Consider the quotient group $G := \mathbb{Q}/\mathbb{Z}$. Show that for all positive integers $m$, we have $mG = G$ and $G\{m\} \cong \mathbb{Z}_m$. From this, conclude that all finite subgroups of $G$ are cyclic.

Exercise 44. Suppose that $G$ is an abelian group that satisfies the following properties:

(i) For all $m$, $G\{m\}$ is either equal to $G$ or is of finite order.

(ii) For some $m$, $\{0\} \subsetneq G\{m\} \subsetneq G$.

Show that $G\{m\}$ is finite for all non-zero $m$.

## Section 8.6

Exercise 45. Let $G$ be a non-trivial, finite abelian group. Let $s$ be the smallest positive integer with the following property: $G = \langle a_1, \ldots, a_s \rangle$ for some $a_1, \ldots, a_s \in G$. Show that $s$ is equal to the value of $t$ in Theorem 8.44. In particular, $G$ is cyclic iff $t = 1$.

Exercise 46. Suppose $G \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_t}$. Let $p$ be a prime, and let $s$ be the number of $m_i$ divisible by $p$. Show that $G\{p\} \cong \mathbb{Z}_p^{\times s}$.

Exercise 47. Suppose $G \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_t}$ with $m_i \mid m_{i+1}$ for $i = 1, \ldots, t-1$, and that $H$ is a subgroup of $G$. Show that $H \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_t}$, where $n_i \mid n_{i+1}$ for $i = 1, \ldots, t-1$ and $n_i \mid m_i$ for $i = 1, \ldots, t$.

Exercise 48. Suppose that $G$ is an abelian group such that for all $m > 0$, we have $mG = G$ and $|G\{m\}| = m^2$. Show that $G\{m\} \cong \mathbb{Z}_m \times \mathbb{Z}_m$ for all $m > 0$. Hint: use induction on the number of prime factors of $m$.

## Section 9.1

Just after Exercise 9.3:

Exercise 49. Let $S$ be an arbitrary, non-empty set, and let $R$ be a ring. As $R$ is an abelian group under addition, we can form the abelian group $\mathrm{Map}(S, R)$ (see Supplementary Exercise 36). We can also equip $\mathrm{Map}(S, R)$ with a multiplication operation: for $f_1, f_2 \in \mathrm{Map}(S, G)$, and for $s \in S$, $(f_1 f_2)(s) := f_1(s) f_2(s)$. Show that $\mathrm{Map}(S, R)$ is a ring.

## Section 9.1.2

Just before Exercise 9.4:

Exercise 50. Suppose that $R$ is a non-trivial ring in which the cancellation law holds: for all $a, b, c \in R$, $a \neq 0_R$ and $ab = ac$ implies $b = c$. Show that $R$ is an integral domain.

## Section 9.2.3

After Exercise 9.12:

Exercise 51. Let $F$ be a finite field of cardinality $q$ and let $t$ be a positive integer. Let $\mathcal{A} := F^{\times t}$ and $\mathcal{Z} := F$. Define a family $\mathcal{H}$ of hash functions from $\mathcal{A}$ to $\mathcal{Z}$ as follows: let $\mathcal{H} := \{h_\alpha : \alpha \in F\}$, where for all $h_\alpha \in \mathcal{H}$ and all $(a_1, \ldots, a_t) \in \mathcal{A}$, we define

$$h_\alpha(a_1, \ldots, a_t) := \sum_{i=1}^{t} a_i \alpha^{i-1} \in \mathcal{Z}.$$

Show that $\mathcal{H}$ is $(t-1)/q$-universal (see Exercise 6.35).

Exercise 52. The purpose of this exercise is to develop a family of hash functions from $\mathcal{A} := \{0,1\}^{\times L}$ to $\mathcal{Z} := \{0,1\}^{\times \ell}$ that is an $\epsilon$-forgeable message authentication scheme with $\epsilon$ very close to the optimal value $1/2^\ell$, while the hash functions have compact descriptions, even when $L$ is significantly larger than $\ell$. More specifically, let $k$ be a positive integer; you are to design a family of hash functions from $\mathcal{A}$ to $\mathcal{Z}$ that is a $(1/2^\ell + L/(k2^k))$-forgeable message authentication scheme, such that each hash function can be described using $O(k+\ell)$ bits.

(a) Let $p$ be a $(k+1)$-bit prime. By breaking up elements of $\mathcal{A}$ into $k$-bit blocks, and interpreting each block as an element of $\mathbb{Z}_p$, construct a $L/(k2^k)$-universal family of hash functions $\mathcal{H}$ from $\mathcal{A}$ to $\mathcal{Y} := \{0,1\}^{\times(k+1)}$, where each element of $\mathcal{H}$ has a $(k+1)$-bit description (see Exercise 6.35 for definitions).

(b) Using the result of Supplementary Exercise 24, describe a pairwise independent family $\mathcal{H}'$ of hash functions from $\mathcal{Y}$ to $\mathcal{Z}$, where each element of $\mathcal{H}'$ has an $O(k+\ell)$-bit description.

(c) Finally, combine $\mathcal{H}$ and $\mathcal{H}'$ as in Exercise 6.40 to obtain the stated result.

The above exercise gives a much better trade-off between forgery rate and hash function size than that given in Exercise 9.24 (later in the text). Supplementary Exercise 94 (below) gives a more elegant construction based on extensions of finite fields. Also note that the above exercise (or Supplementary Exercise 94), combined with Supplementary Exercise 29, gives a method for "extracting" a small amount of high-quality randomness from very long, low-quality strings, using just a small amount of auxiliary randomness.

## Section 9.2.4

Before Exercise 9.19:

EXERCISE 53. Let $R$ be a ring. Show that for $a_1, \ldots, a_n \in R[\mathtt{X}]$, we have

$$\mathbf{D}\Big(\prod_i a_i\Big) = \sum_i \mathbf{D}(a_i) \prod_{j \neq i} a_j$$

and that for $a \in R[\mathtt{X}]$, and $n \geq 1$, we have

$$\mathbf{D}(a^n) = n a^{n-1} \mathbf{D}(a).$$

## Section 9.2.5

EXERCISE 54. Let $R$ be a ring, and consider the ring of multi-variate polynomials $R[\mathtt{X}_1, \ldots, \mathtt{X}_n]$. For $m \geq 0$, define $H_m$ to be the subset of polynomials that can be expresses as a sum of monomials, each of total degree $m$ (by definition, $H_m$ includes the zero polynomial). Polynomials that are sums of monomials of like total degree are called **homogeneous polynomials**. Show that:

(a) if $a, b \in H_m$, then $a + b \in H_m$;

(b) if $a \in H_m$ and $b \in H_n$, then $ab \in H_{m+n}$;

(c) any non-zero polynomial $a$ can be expressed uniquely as $a_0 + \cdots + a_d$, where $a_i \in H_i$ for $i = 0, \ldots, d$, $a_d \neq 0$, and $d = \mathrm{Deg}(a)$;

(d) for any polynomials $a, b$, we have $\mathrm{Deg}(ab) \leq \mathrm{Deg}(a) + \mathrm{Deg}(b)$, and if $R$ is an integral domain, then $\mathrm{Deg}(ab) = \mathrm{Deg}(a) + \mathrm{Deg}(b)$;

(e) if $R$ is an integral domain, and $a, b, c$ are non-zero polynomials such that $a = bc$ and $a$ is homogeneous, then $b$ and $c$ are also homogeneous.

Exercise 55. Prove the "chain rule" for formal derivatives: if $h \in R[\mathtt{Y}_1, ..., \mathtt{Y}_n]$, and $g_1, ..., g_n \in R[\mathtt{X}]$, and $f = h(g_1, ..., g_n) \in R[\mathtt{X}]$, then

$$\mathbf{D}_{\mathtt{X}}(f) = \sum_{i=1}^{n} \mathbf{D}_{\mathtt{Y}_i}(h)(g_1, ..., g_n)\mathbf{D}_{\mathtt{X}}(g_i).$$

## Section 9.3

Before Exercise 9.25:

Exercise 56. Let $a, b$ be elements of a ring $R$. Show that $b \mid a$ iff $a \in bR$ iff $aR \subseteq bR$.

Exercise 57. Let $R$ be a subring of a ring $E$, and let $S := R[\mathtt{X}_1, \ldots, \mathtt{X}_n]$. For $T \subseteq E^{\times n}$, define $I(T)$ to be the set of polynomials $a \in S$ that vanish at all points in $T$, that is, $I(T) := \{a \in S : a(\alpha) = 0 \text{ for all } \alpha \in T\}$. Show that:

(a) $I(T)$ is an ideal of $S$;

(b) if $E$ is an integral domain, and $a^n \in I(T)$ for some positive integer $n$, then $a \in I(T)$.

Exercise 58. Let $R$ be a ring, and $I$ an ideal of $R$. Define $\mathrm{Rad}(I) := \{a \in R : a^n \in I \text{ for some positive integer } n\}$.

(a) Show that $\mathrm{Rad}(I)$ is an ideal. Hint: show that if $a^n \in I$ and $b^m \in I$, then $(a+b)^{n+m} \in I$.

(b) If $R = \mathbb{Z}$ and $I = (d)$, where $d = p_1^{e_1} \cdots p_r^{e_r}$ is the prime factorization of $d$, show that $\mathrm{Rad}(I) = (p_1 \cdots p_r)$.

Just before Exercise 9.31 (and change "following three exercises" above to "following exercises"):

Exercise 59. Let $X, Y, Z$ be subsets of a ring $R$. Show that:

(a) $X \cdot Y$ is closed under addition;

(b) $X \cdot Y = Y \cdot X$;

(c) $X \cdot (Y \cdot Z) = (X \cdot Y) \cdot Z =$ the set of all finite sums of the form $\sum_i x_i y_i z_i$, with $x_i \in X$, $y_i \in Y$, and $z_i \in Z$;

(d) if $X$ an additive subgroup of $R$, then so is $X \cdot Y$;

(e) if $X$ and $Y$ are additive subgroups of $R$, then $(X + Y) \cdot Z = X \cdot Z + Y \cdot Z$.

After Exercise 9.33:

Exercise 60. Let $M$ be a maximal ideal of a ring $R$. Show that for $a, b \in R$, if $ab \in M \cdot M$ and $b \notin M$, then $a \in M \cdot M$.

## Section 9.4

EXERCISE 61. Let $\sigma : R \to R'$ be an embedding of rings, and assume that as sets, $R$ and $R'$ are disjoint. Show that there exists a ring $\hat{R}$, along with a ring isomorphism $\tau : R' \to \hat{R}$, such that $\tau \circ \sigma$ is the identity function. Thus, there is ring isomorphic to $R'$ in which $R$ itself (and not just an isomorphic copy of $R$) is a subring.

EXERCISE 62. Let $F$ be a field, and let $f \in F[\mathtt{X}, \mathtt{Y}]$. Define $V(f) := \{(x, y) \in F \times F : f(x, y) = 0\}$. Let $E := F[\mathtt{X}, \mathtt{Y}]/(f)$.

(a) Any element $\alpha$ of $E$ naturally defines a function from $V(f)$ to $F$, as follows: if $\alpha = [a]_f$, with $a \in F[\mathtt{X}, \mathtt{Y}]$, then for $P = (x, y) \in V(f)$, we define $\alpha(P) := a(x, y)$. Show that this definition is unambiguous, that is, $a \equiv a' \pmod{f}$ implies $a(x, y) = a'(x, y)$.

(b) For $P = (x, y) \in V(f)$, define $M_P := \{\alpha \in E : \alpha(P) = 0\}$. Show that $M_P$ is a maximal ideal of $E$, and that $M_P = [\mathtt{X} - x]_f E + [\mathtt{Y} - y]_f E$.

EXERCISE 63. Continuing with the previous exercise, now assume that the characteristic of $F$ is not 2, and that $f = \mathtt{Y}^2 - g(\mathtt{X})$, where $g \in F[\mathtt{X}]$ is a non-zero polynomial with no multiple roots in $F$.

(a) Show that if $P = (x, y) \in V(f)$, then so is $\bar{P} := (x, -y)$, and that $P = \bar{P}$ iff $y = 0$ iff $g(x) = 0$.

(b) Let $P = (x, y) \in V(f)$. Show that

$$[\mathtt{X} - x]_f E = M_P \cdot M_{\bar{P}}.$$

Hint: treat the cases $P = \bar{P}$ and $P \neq \bar{P}$ separately.

## Section 11.3

It would be better to use the following exercise in place of Exercise 11.14:

EXERCISE 64. Continuing with Exercise 11.13, let $Q'$ be the product of all the primes $q_i$ dividing $p - 1$ with $q_i \leq Y$. Note that $Q' \mid Q$. The goal of this exercise is to estimate the expected value of $\log Q'$, assuming $p$ is a large, random prime. In particular, suppose that $p$ is a random $\ell$-bit prime with $Y \leq 2^{\ell/3}$. Assuming Conjecture 5.24, show that asymptotically (as $\ell \to \infty$), we have

$$\mathsf{E}[\log Q'] = \log Y + O(1).$$

## Section 13.3.1

EXERCISE 65. Let $p$ be a prime with $p \equiv 1 \pmod{4}$.

(a) Using Supplementary Exercise 16, show that there exist positive integers $r, t$, both less than $\sqrt{p}$, such that $r^2 \equiv -t^2 \pmod{p}$; moreover, show how to efficiently compute $r$ and $t$, given $p$.

(b) From part (a), conclude that $p = r^2 + t^2$.

(c) Part (b) says that any prime congruent to 1 modulo 4 is the sum of two squares. Show the converse: any odd prime that is the sum of two squares must be congruent to 1 modulo 4.

### Section 14.1

EXERCISE 66. Let $R$ and $E$ be rings, and $\rho : R \to E$ be a ring homomorphism. Show that using the addition operation of $E$, and defining scalar multiplication by $a \cdot \alpha := \rho(a)\alpha$, we can view $E$ as an $R$-module.

EXERCISE 67. Let $S$ be an arbitrary, non-empty set, and let $M$ be an $R$-module. As $M$ is an abelian group, we can form the abelian group $\mathrm{Map}(S, M)$. We can also equip $\mathrm{Map}(S, M)$ with a scalar multiplication operation: for $f \in \mathrm{Map}(S, G)$, $a \in R$, and $s \in S$, $(af)(s) := a \cdot f(s)$. Show that $\mathrm{Map}(S, M)$ is an $R$-module.

### Section 14.3

EXERCISE 68. Let $M$ and $M'$ be $R$-modules, and consider the $R$-module $\mathrm{Map}(M, M')$, as defined in Supplementary Exercise 67. Let $\mathrm{Hom}_R(M, M')$ be the subset of elements of $\mathrm{Map}(M, M')$ that are $R$-linear maps from $M$ into $M'$. Show that $\mathrm{Hom}_R(M, M')$ is a submodule of $\mathrm{Map}(M, M')$.

### Section 14.4

EXERCISE 69. Show that an $R$-module $M$ has a basis of size $n$ if and only if it is isomorphic to $R^{\times n}$.

### Section 14.5

EXERCISE 70. Let $V$ be a vector space over a field $F$. We can generalize the notion of linear independence and basis to infinite sets, as follows. Let $S$ be a non-empty subset of $V$. Let us say that a function $c : S \to F$ is **zero almost everywhere** if $c(\beta) \neq 0$ for at most finitely many $\beta \in S$, and is **zero everywhere** if $c(\beta) = 0$ for all $\beta \in S$. We say $S$ is **linearly independent** if for any function $c : S \to F$ that is zero almost everywhere, $\sum_{\beta \in S} c(\beta)\beta = 0$ only if $c$ is zero everywhere. We say that $S$ is a basis for $V$ if it is linearly independent, and if for every $\alpha \in V$, there exists a function $c : S \to F$ that is zero almost everywhere and $\sum_{\beta \in S} c(\beta)\beta = \alpha$.

(a) Show that for finite sets $S$, these generalized definitions of linear independence and basis coincide with our original definitions in Section 14.4.

(b) Show that any two bases for $V$ are either both finite and of the same size, or both infinite.

(c) Show that $S$ is basis if and only if it is a maximal linearly independent set (i.e., it is linearly independent, and there is no linearly independent set $S'$ with $S \subsetneq S'$).

(d) It is a fact that any vector space has a (possibly infinite) basis. Prove this fact for vector spaces with a countable number of elements.

Exercise 71. Let $M$ and $M'$ be $R$-modules, and suppose that $\alpha_1, \ldots, \alpha_m$ is a basis for $M$ and $\beta_1, \ldots, \beta_n$ is a basis for $M'$. Consider the $R$-module $\mathrm{Hom}_R(M, M')$ of all $R$-linear maps from $M$ into $M'$ (see Supplementary Exercise 68). For $i = 1, \ldots, m$, let $\pi_i : M \to R$ be the map that sends $\sum_{i=1}^{m} a_i\alpha_i$ to $a_i$, and for $j = 1, \ldots, n$, let $\rho_j : R \to M'$ be the map that sends $a$ to $a\beta_j$. Show that the collection of maps $\rho_j \circ \pi_i$, for $i = 1, \ldots, m$ and $j = 1, \ldots, n$, is a basis for $\mathrm{Hom}_R(M, M')$.

## Section 15.1

Exercise 72. Show that $R^{m\times n}$, using the usual rules for matrix addition and scalar multiplication, is an $R$-module. Furthermore, show that $R^{m\times n}$ has a basis over $R$ of size $mn$.

Exercise 73. Let $A, B \in R^{m\times n}$. Show that if $vA = vB$ for all $v \in R^{1\times m}$, then $A = B$. Also show that if $Aw = Bw$ for all $w \in R^{n\times 1}$, then $A = B$.

Exercise 74. Let $A \in R^{n\times n}$ be a scalar matrix whose diagonal entries are equal to $c \in R$. Show that for all $v \in R^{1\times n}$, we have $vA = cv$ and $Av^\top = cv^\top$.

Exercise 75. Let $A, B \in R^{n\times n}$ be diagonal matrices. Show that $C := AB$ is a diagonal matrix with $C(i, i) = A(i, i)B(i, i)$ for $i = 1, \ldots, n$.

Exercise 76. A matrix $A \in R^{n\times n}$ is called **lower triangular** if $A(i, j) = 0_R$ for $i < j$. Show that the product of two lower triangular matrices is also lower triangular.

## Section 15.2

Exercise 77. Let $M$ and $N$ be $R$-modules, and suppose that $\mathcal{A} = (\alpha_1, \ldots, \alpha_m)$ is an ordered basis for $M$ and $\mathcal{B} = (\beta_1, \ldots, \beta_n)$ be an ordered basis for $N$. Consider the $R$-module $\mathrm{Hom}_R(M, N)$ of all $R$-linear maps from $M$ into $N$ (see Supplementary Exercise 68), and the $R$-module $R^{m\times n}$ (see Supplementary Exercise 72). Let $\Gamma : \mathrm{Hom}_R(M, N) \to R^{m\times n}$ the map that sends $\rho$ to the matrix $T$ that implements the action of $\rho$ with respect to $\mathcal{A}$ and $\mathcal{B}$. Show that $\Gamma$ is an $R$-module isomorphism.

Exercise 78. Let $M$, $N$, and $P$ be $R$-modules, with ordered bases $\mathcal{A} = (\alpha_1, \ldots, \alpha_m)$, $\mathcal{B} = (\beta_1, \ldots, \beta_n)$, and $\mathcal{C} = (\gamma_1, \ldots, \gamma_p)$, respectively. Suppose $\rho : M \to N$ is an $R$-linear map, and that $T \in R^{m\times n}$ is the matrix that implements the action of $\rho$ with respect to $\mathcal{A}$ and $\mathcal{B}$. Also suppose that $\rho' : N \to P$ is an $R$-linear map, and that $T' \in R^{n\times p}$ is the matrix that implements the action of $\rho'$ with respect to $\mathcal{B}$ and $\mathcal{C}$. Show that $TT' \in R^{m\times p}$ is the matrix that implements the action of $\rho' \circ \rho$ with respect to $\mathcal{A}$ and $\mathcal{C}$.

## Section 15.3

**Theorem 15.3.** The following proof may be easier to follow:

> For a matrix $Z \in R^{n\times n}$, let $\sigma_Z$ denote the $R$-linear map that sends $v \in R^{1\times n}$ to $vZ$. So in particular, $\rho = \sigma_A$. Also, let id denote the identity map on $R^{1\times n}$. Evidently, if $I$ is the $n \times n$ identity matrix, then $\sigma_I = \mathrm{id}$; moreover, if $\sigma_Z = \mathrm{id}$, then $Z = I$.

Suppose $A$ is invertible, and let $X \in R^{n\times n}$ be its inverse. Since $AX = I$, we have $\sigma_X \circ \sigma_A = \sigma_I = \mathrm{id}$, and hence $\rho_A$ is injective. Similarly, since $XA = I$, we have $\sigma_A \circ \sigma_X = \sigma_I = \mathrm{id}$, and hence $\rho_A$ is surjective.

Now suppose $\sigma_A$ is bijective. The inverse map $\sigma_A^{-1}$ is also an $R$-module isomorphism. Let $X$ be the matrix representing $\sigma_A^{-1}$ with respect to the standard basis for $R^{1\times n}$. Evidently, $\sigma_X = \sigma_A^{-1}$. If $Y := AX$, then $\sigma_Y = \sigma_X \circ \sigma_A = \sigma_A^{-1} \circ \sigma_A = \mathrm{id}$, from which it follows that $Y = I$. Similarly, if $Z := XA$, then $\sigma_Z = \sigma_A \circ \sigma_X = \sigma_A \circ \sigma_A^{-1} = \mathrm{id}$, from which it follows that $Z = I$.

## Section 15.5

Exercise 79. Let us call a collection of non-zero vectors $v_1, \ldots, v_k \in \mathbb{R}^{1\times m}$ **pairwise orthogonal** if $v_i v_j^\top = 0$ for all $i \neq j$. Show that any pairwise orthogonal collection of vectors over $\mathbb{R}$ is linearly independent.

Exercise 80. The purpose of this exercise is to use linear algebra to prove that any pairwise independent family of hash functions (see §6.7) must contain a large number of hash functions. More precisely, let $\mathcal{H}$ be a pairwise independent family of hash functions from $\mathcal{A}$ to $\mathcal{Z}$, with $|\mathcal{Z}| \geq 2$. Our goal is to show that $|\mathcal{H}| \geq |\mathcal{A}|$. Let $m := |\mathcal{H}|$, $k := |\mathcal{A}|$, and $n := |\mathcal{Z}|$. Write $\mathcal{H} = \{h_1, \ldots, h_m\}$ and $\mathcal{A} = \{a_1, \ldots, a_k\}$. Without loss of generality, we may assume that $\mathcal{Z}$ is a set of non-zero real numbers that sum to zero (e.g., $\mathcal{Z} = \{1, \ldots, n-1, -n(n-1)/2\}$). Now define the matrix $M \in \mathbb{R}^{k\times m}$ with $M(i,j) := h_j(a_i)$. Using the pairwise independence property, show that the rows of $M$ are pairwise orthogonal (see previous exercise), and therefore linearly independent; from this, conclude that $m \geq k$.

## Section 17.3

Exercise 81. Let $a, b \in F[\mathtt{X}]$ be non-zero polynomials, with $m := \deg(a)$ and $n := \deg(b)$. Define

$$\begin{aligned} \tau: \quad F[\mathtt{X}]_{<n} \times F[\mathtt{X}]_{<m} &\to F[\mathtt{X}]_{<m+n} \\ (s,t) &\mapsto as + bt. \end{aligned}$$

Show that $\tau$ is an $F$-linear map, and moreover, that $\tau$ is an $F$-vector space isomorphism if and only if $\gcd(a,b) = 1$.

## Section 17.4

Exercise 82. Let $n_1, \ldots, n_k \in F[\mathtt{X}]$ be non-zero, pairwise relatively prime polynomials and set $n := n_1 \cdots n_k$. Let $\ell_i := \deg(n_i)$ for $i = 1, \ldots, k$, and $\ell := \sum_i \ell_i$. Consider the map

$$\begin{aligned} \tau: \quad F[\mathtt{X}]_{<\ell} &\to F[\mathtt{X}]_{<\ell_1} \times \cdots \times F[\mathtt{X}]_{<\ell_k} \\ a &\mapsto (a \bmod n_1, \ldots, a \bmod n_k). \end{aligned}$$

Show that $\tau$ is an $F$-vector space isomorphism.

## Section 17.6

EXERCISE 83. Consider a field $F$ and its field of rational functions $F(\mathtt{X})$. Let $z \in F(\mathtt{X}) \setminus F$. Show that $\mathtt{X}$ is algebraic over $F(z)$, and that $z$ is transcendental over $F$.

EXERCISE 84. Let $E$ be an extension field of a field $F$. Suppose $\alpha \in E$ is transcendental over $F$, and that $E$ is algebraic over $F(\alpha)$. Show that for any $\beta \in E$, $\beta$ is transcendental over $F$ iff $E$ is algebraic over $F(\beta)$.

EXERCISE 85. Consider $2^{1/2}, 2^{1/3} \in \mathbb{R}$, and the field extensions $\mathbb{Q}[2^{1/2}]$, $\mathbb{Q}[2^{1/3}]$, $\mathbb{Q}[2^{1/2} + 2^{1/3}]$, and $\mathbb{Q}[2^{1/2}][2^{1/3}] = \mathbb{Q}[2^{1/2}, 2^{1/3}] = \mathbb{Q}[2^{1/3}][2^{1/2}]$. Show that:

(a) $(\mathbb{Q}[2^{1/2}] : \mathbb{Q}) = 2$ and $(\mathbb{Q}[2^{1/3}] : \mathbb{Q}) = 3$;

(b) $(\mathbb{Q}[2^{1/2}, 2^{1/3}] : \mathbb{Q}) = 6$;

(c) $\mathbb{Q}[2^{1/2} + 2^{1/3}] = \mathbb{Q}[2^{1/2}, 2^{1/3}]$;

(d) the minimum polynomial of $2^{1/2} + 2^{1/3}$ over $\mathbb{Q}$ has degree 6.

EXERCISE 86. A field $K$ is called **algebraically closed** if every monic polynomial $f \in K[\mathtt{X}]$ splits over $K$ into linear factors, that is, $f = (\mathtt{X} - \alpha_1) \cdots (\mathtt{X} - \alpha_\ell)$, for some $\alpha_1, \ldots, \alpha_\ell \in K$. If, in addition, $K$ is an algebraic extension of a field $F$, then $K$ is called an **algebraic closure** of $F$. Every field $F$ has an essentially unique algebraic closure. This and the following three exercises outline a proof of this; however, to avoid any fancy set theory, we restrict our attention to fields $F$ that are countable (i.e., finite or countably infinite).

(a) Show that a field $K$ is algebraically closed if and only if every non-constant polynomial $f \in K[\mathtt{X}]$ has a root in $K$.

(b) Show that if $E$ is an algebraic extension of a field $K$, then $K$ is not algebraically closed.

(c) Show that any algebraically closed field is infinite.

(d) Show that if a field $F$ is countable, then so is $F[\mathtt{X}]$.

(e) Show that if a field $F$ is countable, and if $K$ is an algebraic extension of $F$, then $K$ is countable.

EXERCISE 87. Let $F_0 \subseteq F_1 \subseteq F_2 \subseteq \cdots$ be a sequence of fields such that $F_0 := F$ and $F_{i+1}$ is an extension of $F_i$ for each $i \geq 0$. Set $E := \cup_{i \geq 0} F_i$. We can naturally define addition and multiplication on $E$ as follows: for $a, b \in E$, there is some $i \geq 0$ for which $F_i$ contains both $a$ and $b$, and we define $a + b$ and $ab$ using the rules for addition and multiplication in $F_i$. Show that this definition is unambiguous (i.e., it does not depend on the choice of $i$), and that it makes $E$ into a field. Moreover, show that if each extension $F_{i+1}$ is algebraic over $F_i$, then $E$ is algebraic over $F$.

EXERCISE 88. This exercise proves the existence of algebraic closures.

(a) Let $F$ be any countable field. Let $f_1, f_2, f_3 \ldots$ be an enumeration of all monic polynomials in $F[\mathtt{X}]$ (by part (d) of Supplementary Exercise 86, $F[\mathtt{X}]$ is countable). Set $F_0 := F$, and for each $i \geq 0$, let $F_{i+1}$ be a finite extension of $F_i$ over which $f_{i+1}$ splits into linear factors (as in Theorem 17.19). Set $F_* := \cup_{i \geq 0} F_i$ (with addition and multiplication defined as in Supplementary Exercise 87). Show that $F_*$ is a field that is algebraic over $F$, and that all monic polynomials $f \in F[\mathtt{X}]$ split into linear factors over $F_*$.

(b) Let $F$ be any countable field. Define the sequence of extension fields $F^{(0)} \subseteq F^{(1)} \subseteq F^{(2)} \subseteq \ldots$, where $F^{(0)} := F$, and $F^{(i+1)} := (F^{(i)})_*$ for $i \geq 0$ (as defined in part (a)). Set $K := \cup_{i \geq 0} F^{(i)}$ (with addition and multiplication defined as in Supplementary Exercise 87). Show that $K$ is an algebraic closure of $F$.

Exercise 89. This exercise proves the uniqueness of algebraic closures. Let $F$ be a field, and let $K$ and $K'$ be two algebraic closures of $F$.

(a) For $\alpha \in K$, show that there is an embedding $\sigma : F[\alpha] \to K'$ that leaves $F$ fixed (i.e., the restriction of $\sigma$ to $F$ is the identity map).

(b) Generalizing part (a), suppose that $E$ is a subfield of $K$ containing $F$, that $\sigma : E \to K'$ is an embedding, and that $\alpha \in K$. Show how to extend $\sigma$ to an embedding $\sigma' : E[\alpha] \to K'$ (i.e., $\sigma'$ should agree with $\sigma$ on $E$).

(c) Using the result of part (b), and assuming $F$ is countable, show that there exists an embedding $\tau : K \to K'$ that leaves $F$ fixed.

(d) Show that any embedding $\tau$ as in part (c) must in fact be surjective. Conclude that any two algebraic closures of $F$ are isomorphic as $F$-algebras.

Note that the field $\mathbb{C}$ of complex numbers is algebraically closed (although this is by no means obvious).

## Section 17.8.1

The following exercises can replace and augment Exercise 17.35. They develop more fully divisibility properties in $\mathbb{Z}[i]$.

Exercise 90. Let $\delta \in \mathbb{Z}[i]$. Show that:

(a) if $\delta$ is irreducible in $\mathbb{Z}[i]$, then so is its complex conjugate $\bar{\delta}$;

(b) if $N(\delta)$ is a prime number, then $\delta$ is irreducible in $\mathbb{Z}[i]$;

(c) if $\delta$ is irreducible in $\mathbb{Z}[i]$, then $N(\delta)$ is of the form $p$ or $p^2$ for some prime number $p$.

Exercise 91. In Exercise 17.32, we saw that 2 factors as $-i\pi^2$ in $\mathbb{Z}[i]$, where $\pi := 1 + i$ is irreducible. The exercise examines the factorization in $\mathbb{Z}[i]$ of primes $p > 2$.

(a) Show that either $p$ is irreducible in $\mathbb{Z}[i]$, or $p$ splits in $\mathbb{Z}[i]$ as $p = \delta\bar{\delta}$, where $\delta \in \mathbb{Z}[i]$ is irreducible, and the complex conjugate $\bar{\delta}$ (which is also irreducible) is not associate to $\delta$.

(b) Show that if $p$ splits in $\mathbb{Z}[i]$, then $p \equiv 1 \pmod 4$.

(c) Show that if $p \equiv 1 \pmod 4$, then $p$ splits in $\mathbb{Z}[i]$; in particular, show that if $c \in \mathbb{Z}$ with $c^2 \equiv -1 \pmod p$, then $p = \delta\bar{\delta}$ where $\delta$ is a greatest common divisor (in $\mathbb{Z}[i]$) of $c + i$ and $p$.

Note that the above Supplementary Exercise can be solved without using the results of Supplementary Exercise 65, and indeed, yields an alternative proof of the same result.

## Section 18.3

Exercise 92. Let $a, b \in F[\mathtt{X}]$, with $\deg(a) \geq \deg(b) \geq 0$, let $d := \gcd(a, b)$, and let $q := a/d$. Show that Euclid's algorithm on inputs $a$ and $b$ uses $O(\operatorname{len}(b)\operatorname{len}(q))$ operations in $F$.

## Section 19.3

**Theorem 19.3.** A simpler proof runs as follows:

> By Theorem 14.26, we can extend $\delta_1, \ldots, \delta_m$ to an ordered basis $\delta_1, \ldots, \delta_m, \delta_{m+1}, \ldots, \delta_\ell$. Now choose $\pi$ to be the element of $\mathcal{D}_F(V)$ whose coordinate vector, with respect to this ordered basis, is $a_1, \ldots, a_m, a_{m+1}, \ldots, a_\ell$, where $a_{m+1}, \ldots, a_\ell \in F$ are arbitrary.

## Section 20.2

Exercise 93. As an alternative to the approach taken in Supplementary Exercise 52, extensions of finite fields can be used to design a very elegant, compact, and effective message authentication scheme. Let $F$ be a finite field of cardinality $q$, and let $t$ and $m$ be positive integers. Let $\mathcal{A} := F^{\times t}$ and $Z := F$. Show how to construct a family $\mathcal{H}$ of hash from $\mathcal{A}$ to $\mathcal{Z}$ so that (i) $\mathcal{H}$ is in one-to-one correspondence with $F^{\times(2m+1)}$, and (ii) $\mathcal{H}$ is an $\epsilon$-forgeable message authentication scheme, where $\epsilon = 1/q + t/(mq^m)$. Hint: making use of an irreducible polynomial of degree $m$ over $F$, along with the result of Exercise 6.40, show how to combine a $t/(mq^m)$-universal family of hash function from $F^{\times t}$ to $F^{\times m}$ with a pairwise independent family of hash functions from $F^{\times m}$ to $F$.

## Section 20.3

Exercise 94. Let $F$ be a finite field of cardinality $q$. This exercise develops an alternative construction of an algebraic closure of $F$ (see Supplementary Exercises 86–89). Show that there exists a sequence of fields $F_1 \subseteq F_2 \subseteq F_3 \cdots$ such that $F_1 = F$, and for $i \geq 2$, $F_i$ is a degree $i$ extension of $F_{i-1}$. Set $E := \cup_{i \geq 1} F_i$ (with addition and multiplication defined as in Supplementary Exercise 87). Show that $E$ is an algebraic closure of $F$.

## Section 21.3

**Theorem 21.4.** The following is a cleaner proof:

We may assume $r \geq 2$. Let $N$ be a random variable that denotes the number of iterations of the main loop of the algorithm. For $n = 1, \ldots, N$, let $H_n$ denote the value of $H$ at the beginning of loop iteration $n$. For $i, j = 1, \ldots, r$, we define $N_{ij}$ to be the largest value of $n$ (with $1 \leq n \leq N$) such that $g_i \mid h$ and $g_j \mid h$ for some $h \in H_n$.

We first claim that $\mathsf{E}[N] = O(\operatorname{len}(r))$. To prove this claim, we make use of the fact (see Theorem 6.25) that

$$\mathsf{E}[N] = \sum_{n \geq 1} \mathsf{P}[N \geq n].$$

Now, $N \geq n$ if and only if for some $i, j$ with $1 \leq i < j \leq r$, we have $N_{ij} \geq n$. Moreover, if $g_i$ and $g_j$ have not been separated at the beginning of one loop iteration, then they will be separated at the beginning of the next with probability $1/2$. It follows that

$$\mathsf{P}[N_{ij} \geq n] = 2^{-(n-1)}.$$

So we have

$$\mathsf{P}[N \geq n] \leq \sum_{i<j} \mathsf{P}[N_{ij} \geq n] \leq r^2 2^{-n}.$$

Therefore,

$$\begin{aligned}\mathsf{E}[N] &= \sum_{n \geq 1} \mathsf{P}[N \geq n] = \sum_{n \leq 2\log_2 r} \mathsf{P}[N \geq n] + \sum_{n > 2\log_2 r} \mathsf{P}[N \geq n] \\ &\leq 2\log_2 r + \sum_{n > 2\log_2 r} r^2 2^{-n} \leq 2\log_2 r + \sum_{n \geq 0} 2^{-n} = 2\log_2 r + 2,\end{aligned}$$

which proves the claim.

As discussed in the paragraph above this theorem, the cost of each iteration of the main loop is $O(k\ell^2 \operatorname{len}(q))$ operations in $F$. Combining this with the fact that $\mathsf{E}[N] = O(\operatorname{len}(r))$, it follows that the expected number of operations in $F$ for the entire algorithm is $O(\operatorname{len}(r)k\ell^2 \operatorname{len}(q))$. This is significantly better than the above quick-and-dirty estimate, but is not quite the result we are after. For this, we have to work a little harder.

For any polynomial $h$ dividing $g$, define $\omega(h)$ to be the number of irreducible factors of $h$. Let us also define

$$S := \sum_{n=1}^{N} \sum_{h \in H_n} \omega(h)^2.$$

It is easy to see that the total number of operations performed by the algorithm is $O(Sk^3 \operatorname{len}(q))$, and so it will suffice to show that $\mathsf{E}[S] = O(r^2)$.

We claim that

$$S = \sum_{i,j} N_{ij},$$

where the sum is over all $i, j = 1, \ldots, r$. To see this, define $I_{ij}(h)$ to be 1 if both $g_i$ and $g_j$ divide $h$, and 0 otherwise. Then we have

$$S = \sum_n \sum_{h \in H_n} \sum_{i,j} I_{ij}(h) = \sum_{i,j} \sum_n \sum_{h \in H_n} I_{ij}(h) = \sum_{i,j} N_{ij},$$

which proves the claim.

We can write

$$S = \sum_{i \neq j} N_{ij} + \sum_i N_{ii} = \sum_{i \neq j} N_{ij} + rN.$$

For $i \neq j$, we have

$$\mathsf{E}[N_{ij}] = \sum_{n \geq 1} \mathsf{P}[N_{ij} \geq n] = \sum_{i \geq 1} 2^{-(n-1)} = 2,$$

and so

$$\mathsf{E}[S] = \sum_{i \neq j} \mathsf{E}[N_{ij}] + r\mathsf{E}[N] = 2r(r-1) + O(r \operatorname{len}(r)) = O(r^2).$$

That proves the theorem.

Additional exercises for this section:

Exercise 95. Suppose that in Algorithm EDF, we replace the two lines

```
for each $h \in H$ do
    choose $\alpha \in F[\mathtt{X}]/(h)$ at random
```

by the following:

```
choose $a \in F[\mathtt{X}]_{<2k}$ at random
for each $h \in H$ do
    $\alpha \leftarrow [a]_h \in F[\mathtt{X}]/(h)$
```

Show that the expected running time bound of Theorem 21.4 still holds (you may assume $p = 2$ for simplicity).