Solutions to Ireland, Rosen "A Classical Introduction to Modern Number Theory"

Adam Michalik

9 maja 2017

1 Chapter 1

Ex. 1.1 Let a and b be nonzero integers. We can find nonzero integers q and r such that $a = qb + r$ where $0 \leqslant r < b$. Prove that $(a, b) = (b, r)$

As a reminder, $(a_1, \ldots, a_n)$ is defined to be the ideal generated by a_i, but also sometimes by abuse of notation it denotes the smallest positve member of the ideal (which generates it).

The relation $a = qb + r$ shows that $a \in (b, r)$, so $(a, b) \subset (b, r)$. On the other hand, $r = qb - a$, so $r \in (a, b)$, whus $(r, b) \subset (a, b)$.

Ex. 1.2 XXX Exercise statement missing.

The only thing here that needs proving is that the process finishes in finitely many steps, but this is clear, as $r_i > r_{i+1} \geqslant 0$ by construction, so r_i is a decreasing sequence of real numbers, which cannot be infinite.

Ex. 1.3 Calculate $(187, 221)$, $(6188, 4709)$, $(314, 159)$.

Use the method from Ex. 1.2. Calculation omitted.

Ex. 1.4 Let $d = (a, b)$. Show how one can use the Euclidean algorithm to find numbers m and n such that $am + bn = d$.

The method from Ex. 1.2 produces a sequence r_i, such that $r_{k+1} = d$, and $r_{k+2} = 0$, that is, $r_{k+1} | r_k$. We have

$$r_{k-1} = q_{k+1} r_k + r_{k+1}, \tag{1}$$

so

$$r_{k+1} = r_{k-1} - q_{k+1} r_k. \tag{2}$$

Next, we have

$$r_{k-2} = q_k r_{k-1} + r_k, \tag{3}$$

so

$$r_k = r_{k-2} - q_k r_{k-1}. \tag{4}$$

Substituting (4) back to (2) allows us to express $d = r_{k+1}$ in terms of r_{k-1}, r_{k-2}. Continuing this procedure will allow us to express d in terms of r_i, r_{i-1}, and finally in terms of r_1, r_0, which can be expressed in terms of a and b.

Ex. 1.5 Find m and n for the pairs a and b given in Ex 1.3

Skipped.

Ex. 1.6 Let $a, b, c \in \mathbb{Z}$. Show that the equation

$$ax + by = c \tag{5}$$

has solutions in integers iff $(a, b) | c$.

From $ax + by = c$ it instantly follows that any common divisor of a and b also divides c, so $(a, b) | c$. On the other hand, if $(a, b) | c$, let $d = (a, b)$, and write $c = dd'$ for $d' \in \mathbb{Z}$. Write $am + bn = d$ for $m, n \in \mathbb{Z}$. Multiplying by d' gives us $amd' + bnd' = dd' = c$. We see that this gives a solution to (5) – set $x = md', y = nd'$.

Ex. 1.7 Let $d = (a, b)$ and $a = da'$ and $b = db'$. Show that $(a', b') = 1$.

Let $d'|a'$. Since $a = da'$, this means that $d'd|a$. Similarly, if $d'|b'$, we show that that $d'd|b$. This gives us $d' = 1$ – otherwise, $d'd$ would have been a greater common divisor of a, b.

Ex. 1.8 Let x_0 and y_0 be a solution to $ax+by = c$. Show that all solutions have the form $x = x_0+t(b/d)$, $y = y_0 - t(a/d)$, where $d = (a, b)$ and $t \in \mathbb{Z}$.

We have $a(x - x_0) + b(y - y_0) = 0$. Clearly, $a/d|a(x - x_0)$, so also $a/d|b(y - y_0)$. Since $(b/d, a/d) = 1$ by previous exercise, we also $(b, a/d) = 1$, therefore a/d must divide $y - y_0$. Similarly, b/d must divide $x - x_0$. Let $x - x_0 = t(b/d), y - y_0 = t'(a/d)$. We have $at(b/d) + bt'(a/d) = 0$, so $t' = -t$.

Ex. 1.9 Suppose that $u, v \in \mathbb{Z}$ and that $(u, v) = 1$. If $u|n$ and $v|n$, show that $uv|n$. Show that this is false if $(u, v) \neq 1$.

If $(u, v) = d \neq 1$, let $n = u(v/d) = (u/d)v$. Clearly $u|n$ and $v|n$. On the other hand, $uv > n$, so it cannot divide n.

Now let $(u, v) = 1$, and $u|n$, $v|n$. Write $n = au = bv$. Since $v|n$, $v|au$. Since $(u, v) = 1$, by proposition 1.1.1, $v|a$, that is, $a = a'v$. Thus, $n = a'vu$, so $vu|n$.

Ex. 1.10 Suppose that $(u, v) = 1$. Show that $(u + v, u - v)$ is either 1 or 2.

Let $d = (u+v, u-v)$. Since $d|u+v$ and $d|u-v$, by taking sum and difference, $d|2u$ and $d|2v$. Take any prime $p|d$, it also divides both $2u$ and $2v$. If $p > 2$, by proposition 1.1.1, $p|u$ and $p|v$, which contradicts $(u, v) = 1$.

Ex. 1.11 Show that $(a, a + k)|k$.

Let $d|a$, $d|a + k$. It also must divide their difference, that is, $a + k - a = k$.

Ex. 1.12 Suppose that we take several copies of a regular polygon and try to fit them evenly about a common vertex. Prove that the only possibilities are six equilateral triangles, four squares, and three hexagons.

Consider an arrangment of k n-gons evenly about a common vertex. The sum internal angle in a regular n-gon is $\pi - 2\pi/n = (n-2)\pi/n$. Thefore, we must have $2\pi = k(n-2)\pi/n$, so $2n = k(n-2)$, thus $2n + 2k = kn$. By symmetry, we can assume that $n \leqslant k$. Then, $kn = 2k + 2n \leqslant 2k + 2k = 4k$, so $n \leqslant 4$, and thus $n = 3$ and $k = 6$, or $n = 4$ and $k = 4$. From the symmetrical case, we get $k = 3$, $n = 6$.

Ex. 1.13 Skipped.

Ex. 1.14 Skipped.

Ex. 1.15 Prove that $a \in \mathbb{Z}$ is the square of another integer iff $ord_p(a)$ is even for all primes p. Give a generalization.

A generalization is of course "a is n-th power if $ord_p(a)$ is divisible by n for all primes p. There's a slight error in the question – one also needs to look at the sign of a – -4 is not a square of another integer, even though $ord_p(a)$ is even for all primes p. We'll therefore assume that $a \in \mathbb{N}$.

The exercise is obvious once we look at the unique factorization – we have:

$$a = \prod_{p|a,\, p \text{ prime}} p^{ord_p(a)} \tag{6}$$

Since $ord_p(a)$ are even, $ord_p(a)/2$ are integers, so:

$$a = \prod_{p|a,\, p \text{ prime}} (p^{ord_p(a)/2})^2 = \left(\prod_{p|a,\, p \text{ prime}} p^{ord_p(a)/2} \right)^2 \tag{7}$$

For the other direction, if $a = b^2$, then clearly $ord_p(a) = 2ord_p(b)$. The proof generalizes for $n > 2$.

Ex. 1.16 If $(u, v) = 1$ and $uv = a^2$, show that both u and v are squares.

By previous exercise, and by symmetry, it's enough to prove that $ord_p(u)$ is even. Now, $ord_p(a^2) = ord_p(u)+ord_p(v)$, so $2ord_p(a) = ord_p(u)+ord_p(v)$. One of $ord_p(u), ord_p(v)$ must be 0, otherwise p divides both u and v, which contradicts $(u, v) = 1$. Thus, either $ord_p(u) = 0$, which is even, or $ord_p(u) = 2ord_p(a)$, which is even too.

Ex. 1.17 Prove that the square root of 2 is irrational, i.e., that there is no rational number $r = a/b$ such that $r^2 = 2$.

Follows from Ex 1.18

Ex. 1.18 Prove that $\sqrt[n]{m}$ is irrational if m is not the n-th power of an integer.

Let $r = a/b$ be such that $r^n = m$. Assume r is in lowest terms, that is, $(a, b) = 1$. It necessarily follows that $(a^n, b^n) = 1$, so $m = r^n = a^n/b^n$ is also in lowest terms. Thus, if m is an integer, $b^n = 1$, so $b = 1$, and r is also an integer.

Ex. 1.19 Define the least common multiple of two integers a and b to be an integer m such that $a|m$, $b|m$, and m divides every common multiple of a and b. Show that such an m exists. It is determined up to sign. We shall denote it by $[a, b]$.

Consider a set $I = \{n \in \mathbb{Z} : a|n \wedge b|n\}$. Clearly it is an ideal of $\mathbb{Z}$, and so $I = (m)$ for some m.

Ex. 1.20 Skipped.

Ex. 1.21 Skipped.

Ex. 1.22 Skipped.

Ex. 1.23 Suppose that $a^2 + b^2 = c^2$ with $a, b, c \in \mathbb{Z}$ For example, $3^2 + 4^2 = 5^2$ and $5^2 + 12^2 = 13^2$. Assume that $(a, b) = (b, c) = (c, a) = 1$. Prove that there exist integers u and v such that $c - b = 2u^2$ and $c + b = 2v^2$ and $(u, v) = 1$ (there is no loss in generality in assuming that b and c are odd and that a is even). Consequently $a = 2uv$, $b = v^2 - u^2$, and $c = v^2 + u^2$. Conversely show that if u and v are given, then the three numbers a, b, and c given by these formulas satisfy $a^2 + b^2 = c^2$.

If $a^2+b^2 = c^2$, we have $a^2 = c^2-b^2 = (c-b)(c+b)$. By Ex 1.10, $(c-b, c+b)$ is either 1 or 2. Since both b, c are odd, both $c-b, c+b$ are even, and so $(c-b, c+b) = 2$. Thus, $c-b = 2x$, $c+b = 2y$, and $(x, y) = 1$. Consider any prime $p \neq 2$. As $a^2 = c^2-b^2 = (c-b)(c+b)$, and $ord_p(c-b) = ord_p(x), ord_p(c+b) = ord_p(y)$ for $p \neq 2$, it follows that $2ord_p(a) = ord_p(c - b) + ord_p(c + b) = ord_p(x) + ord_p(y)$, and one of the $ord_p(x), ord_p(y)$ must be 0, as $(x, y) = 1$. Thus $ord_p(x)$ and $ord_p(y)$ are even for all p, and so $x = u^2$, $y = v^2$.

The other direction is simple calculation.

Ex. 1.24 Skipped.

Ex. 1.25 If $a^n - 1$ is a prime, show that $a = 2$ and that n is a prime. Primes of the form $2^p - 1$ are called Mersenne primes. For example, $2^3 - 1 = 7$ and $2^5 - 1 = 31$. It is not known if there are infinitely many Mersenne primes.

Let $a^n - 1$ be prime. We have:

$$a^n - 1 = (a - 1)(a^{n-1} + a^{n-2} + \ldots + a + 1) \tag{8}$$

It follows that $a - 1|a^n - 1$, but as $a^n - 1$ is prime, $a - 1 = 1$, and so $a = 2$.

Similarly, let $n = uv$, and let $u \leqslant v$. We have:

$$2^n - 1 = 2^{uv} - 1 = (2^u)^v - 1 = (2^u - 1)((2^u)^{v-1} + (2^u)^{v-2} + \ldots + 2^u + 1) \tag{9}$$

We thus have that $2^u - 1|2^n - 1$, but since $2^n - 1$ is prime, $2^u - 1 = 1$, so $u = 1$, and therfore n is prime.

Ex. 1.26 If $a^n + 1$ is a prime, show that a is even and that n is a power of 2. Primes of the form $2^{2^t} + 1$ are called Fermat primes. For example, $2^{2^1} + 1 = 5$ and $2^{2^2} + 1 = 17$. It is not known if there are infinitely many Fermat primes.

Let $a^n + 1$ be prime. If a is odd, $a^n + 1$ is even, so it is prime only if $a = n = 1$ (this is a minor mistake in the statement of the problem). Assume now that a is even. Suppose that $p|n$, p is odd. Then, letting $n = pv$ for some v, we have:

$$a^n + 1 = a^{pv} + 1 = (a^v)^p + 1 = (a^v + 1)((a^u)^{p-1} + (a^v)^{p-2} + \ldots + a^v + 1) \tag{10}$$

So, $a^v + 1|a^n + 1$, and therefore $a^n + 1$ is not prime.

Ex. 1.27 For all odd n show that $8|n^2-1$. If 3 doesn't divide n, show that $6|n^2-1$.

We have $n^2-1=(n+1)(n-1)$. Since n is odd, both $n+1, n-1$ are even, and moreso, one of these must be divisible by 4, as one of the two consecutive odd numbers is divisible by 4. Thus, their product is divisible by 8. Similarly, if 3 does not divide n, it must divide one of $n-1, n+1$, otherwise it wouldn't divide three consecutive integers, which is impossible. As n is odd, $n+1$ is even, so $(n+1)(n-1)$ is divisible by both 2 and 3, so it is divisible by 6.

Ex. 1.28 For all n show that $30|n^5-n$ and that $42|n^7-n$.

The reasoning here is very similar to the previous exercise – for the first, we use $30=2\cdot 3\cdot 5$ with $n^5-n=n(n^4-1)=n(n^2-1)(n^2+1)=n(n-1)(n+1)(n^2+1)$. It necessarily follows that one of $n-1, n, n+1$ is divisible by 2, one by 3, and if none of them is divisible by 5, it follows that n gives the remainder of 2 or 3 when divided by 5. But then, n^2 gives the rest of $2^2=4$ in the first case, and 3^2 mod $5=4$ in the second case, so in both cases n^2+1 is divisible by 5. We omit the similar argument for $42|n^7-n=n(n^6-1)=n(n^2-1)(n^2+n+1)$.

Ex. 1.29 Suppose that $a,b,c,d\in\mathbb{Z}$ and that $(a,b)=(c,d)=1$. If $(a/b)+(c/d)=$ an integer, show that $b=d$ or $b=-d$.

We have:

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd} \tag{11}$$

Assume that it is an integer, that is, $bd|ad+bc$. Since $d|bd$ and $d|ad$, we also have $d|bc$, but $(c,d)=1$, so $d|b$. Similarly we argue that $b|d$. The thesis follows.

Ex. 1.30 Prove that

$$H_n=1+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{n} \tag{12}$$

is not an integer.

Let 2^s be the largest power of 2 occuring as a denominator in H_n, say $2^s=k\leqslant n$. Write $H_n=\frac{1}{2^s}+(1+1/2+\ldots+1/(k-1)+1/(k+1)+\ldots+1/n$. The sum in parentheses can be written as $1/2^{s-1}$ times sum of fractions with odd denominators, so the denominator of the sum in parentheses will not be divisible by 2^s, but it must equal 2^s by Ex 1.29.

Ex. 1.31 Show that 2 is divisible by $(1+i)^2$ in $\mathbb{Z}[i]$.

We have $(1+i)^2=1+2i-1=2i$, so $2=-i(1+i)^2$.

Ex. 1.32 For $\alpha=a+bi\in\mathbb{Z}[i]$ we defined $\lambda(\alpha)=a^2+b^2$. From the properties of λ deduce the identity $(a^2+b^2)(c^2+d^2)=(ac-bd)^2+(ad+bc)^2$.

It is not clear what exactly properties of λ they mean, but most likely the fact that $\lambda(ab)=\lambda(a)\lambda(b)$, which is never stated in the text, but amounts to proving this very identity.

Ex. 1.33 Show that $\alpha\in\mathbb{Z}[i]$ is a unit iff $\lambda(\alpha)=1$. Deduce that 1, -1, i, and - i are the only units in $\mathbb{Z}[i]$.

If $\lambda\alpha=1$, then we must have $a^2+b^2=1$, and so either $a^2=1, b^2=0$, in which case either $a=1$ or $a=-1$, or $a^2=0, b^2=1$, in which case $b=1$ or $b=-1$. These 4 options give us $1,-1,i,-i$, all of which are units of $\mathbb{Z}[i]$.

In the other direction, let α be a unit, that is, there exists β such that $\alpha\beta=1$. We have $1=\lambda(1)=\lambda(\alpha\beta)=\lambda(\alpha)\lambda(\beta)$, and so $\lambda(\alpha)=1$.

Ex. 1.34 Show that 3 is divisible by $(1-\omega)^2$ in $\mathbb{Z}[\omega]$.

We have $(1-\omega)^2=1-2\omega+\omega^2$. Now, $\omega=(-1+\sqrt{-3})/2$ and $\bar{\omega}=\omega^2$, so $1-2\omega+\omega^2=2-\sqrt{-3}+(-1-\sqrt{-3})/2=3(1-\sqrt{3})/2=3\cdot(-\omega)$. Now, ω is a unit of $\mathbb{Z}[\omega]$, so $3=-(1-\omega)^2\cdot\omega^{-1}$

Ex. 1.34 For $\alpha = a + b\omega \in \mathbb{Z}[\omega]$ we defined $\lambda(\alpha) = a^2 - ab + b^2$. Show that α is a unit iff $\lambda(\alpha) = 1$. Deduce that $1, -1, \omega, -\omega, \omega^2, and - \omega^2$ are the only units in $\mathbb{Z}[\omega]$.

It is enough to show that λ is multiplicative. We have:

$$\alpha = a + b\omega = (2a - b)/2 + ib\sqrt{3}/2 \tag{13}$$

Thus $|\alpha|^2 = (4a^2 - 4ab + b^2)/4 + 3b^2/4 = a^2 - ab + b^2$, so λ coincides with square of complex absolute value, which is multiplicative.

Ex. 1.39 Show that in any integral domain a prime element is irreducible.

Let p be a prime element of A, that is, $(p) \subset A$ is a prime ideal. Suppose $p = ab$. Since $ab \in (p)$, and (p) is prime, either a or b is in (p), say a. Then $a = px$ for some $x \in A$. We then have $p = ab = pxb$, so $p(1 - bx) = 0$. Since A is integral domain, $1 - bx = 0$, so $1 = bx$, that is, b is a unit, and therefore p is irreducible.

2 Chapter 2

Ex. 2.1 Show that $k[x]$, with k a finite field, has infinitely many irreducible polynomials.

Let $f_1, \ldots, f_n$ be a finite set of polynomials in $k[x]$. Consider $f = 1 + \prod f_i$. It is not divisible by any of f_i, so none of its irreducible factors can be equal to any of the f_i. Therefore $f_1, \ldots, f_n$ is not the list of all irreducible polynomials in $k[x]$.

Ex. 2.2 The ring is just a localization of $\mathbb{Z}$ at $\prod(p_i) = (\prod p_i)$. This corresponds to affine subscheme of $\operatorname{Spec}\mathbb{Z}$ consisting of points (p_i).

Ex. 2.3 Use the formula for $\phi(n)$ to give a proof that there are infinitely many primes.

Let $p_1, \ldots, p_t$ be all primes. Consider $n = \prod p_i$. Then $\phi(n) = n\prod(1 - 1/p_i) = n\prod(p_i - 1)/p_i = \prod(p_i - 1)$. Since 3 is prime, $\phi(n) > 1$, but this means that there exists $1 \leqslant k < n$ that is relatively prime to n, but this is impossible, as any of its prime factors must also be a factor of n.

Ex. 2.4 If a is a nonzero integer, then for $n > m$ show that $(a^{2^n} + 1, a^{2^m} + 1) = 1$ or 2 depending on whether a is odd or even.

First we'll prove that if a prime p divides $a^{2^m} + 1$, it must also divide $a^{2^n} - 1$ for all $n > m$. This is simple induction: for $n = m + 1$, we have $p|a^{2^m} + 1|(a^{2^m} + 1)(a^{2^m} - 1) = (a^{2^m})^2 - 1 = a^{2^{m+1}} - 1$. The induction step is similar.

Thus, if p divides both $a^{2^n} + 1, a^{2^m} + 1$ for $n > m$, it also divides $a^{2^n} - 1$ by reasoning above, so it must divide the difference $a^{2^n} + 1 - (a^{2^n} - 1) = 2$. This means that p must be 2. It is easy to see that this will be the case whenever a is odd – in that case, both $a^{2^n} + 1, a^{2^m} + 1$ will be even.

Ex. 2.5 Use the result of Ex. 2.4 to show that there are infinitely many primes.

Clearly, since $(2^{2^n} + 1, 2^{2^m} + 1) = 1$, all of the prime factors of $2^{2^n} + 1$ are different from all of the prime factors of $2^{2^m} + 1$ for $n \neq m$ Since there are infinitely many numbers of the form $2^{2^n} + 1$, there must be infinitely many primes.

Ex. 2.6 For a rational number r let $[r]$ be the largest integer less than or equal to r, e.g., $[1/2] = 0$, $[2] = 2$, and $[3 + 1/3] = 3$. Prove $ord_p n! = [n/p] + [n/p^2] + [n/p^3] + \ldots$.

Since $n!$ is a product of $1, 2, 3, \ldots, n$, every p-th integer contribute a factor of p to the whole product, which correspond to the $[n/p]$ summand in the formula, every p^2-th factor contributes another p factor to the product, which corresponds to $[n/p^2]$ summand, etc.

Ex. 2.7 Deduce from Ex. 2.6 that $ord_p n! \leqslant n/(p - 1)$ and that $\sqrt[n]{n!} \leqslant \prod_{p|n!} p^{1/(p-1)}$.

We have:

$$ord_p n! = [n/p] + [n/p^2] + [n/p^3] + \ldots \leqslant n/p + n/p^2 + \ldots = \frac{n}{p}\sum_{i=0} 1/p^i = \frac{n}{p}\frac{1}{1 - 1/p} = \frac{n}{p - 1} \tag{14}$$

The inequality $\sqrt[n]{n!} \leqslant \prod_{p|n!} p^{1/(p-1)}$ is equivalent to $n! \leqslant \prod_{p|n!} p^{n/(p-1)}$, which is easily derived by using the previous inequality to an equality:

$$m = \prod_{p|m} p^{ord_p m} \tag{15}$$

Ex. 2.7 Use Exercise 7 to show that there are infinitely many primes.

Let $p_1, \ldots, p_n$ be all primes. Then $\sqrt[n]{n!} \leqslant \prod_{p|n!} p^{1/(p-1)} \leqslant \prod_i p_i^{1/(p_i-1)}$, which is independent of n. This implies that $\sqrt{n}n!$ is a bounded sequence. However, $(n!)^2 \geqslant n^n$ – this is seen by noting that $(n!)^2 = \prod_{1 \leqslant i \leqslant n} i(n-i+1)$, and for $1 \leqslant i \leqslant n$, $i(n-i+1) \geqslant n$ - indeed, a quadratic function $-i^2 + i(n+1)$ attains maximum for $i = (n+1)/2$, and is monotonically decreasing in both directions, while still being no smaller than n for both $i = 1$ and $i = n$.

Therefore, $\sqrt[n]{(n!)} \geqslant \sqrt{n}$, but $\sqrt{n}$ is unbounded, which is a contradiction with boundedness of $\sqrt[n]{(n!)}$.

Ex. 2.8 A function on the integers is said to be multiplicative if $f(ab) = f(a)f(b)$. whenever $(a, b) = 1$. Show that a multiplicative function is completely determined by its value on prime powers.

Trivial.

Ex. 2.9 If $f(n)$ is a multiplicative function, show that the function $g(n) = \sum_{d|n} f(d)$ is also multiplicative.

We'll prove a stronger theorem, that is, if f and g are multiplicative functions, then their Dirichlet product is also a multiplicative function.

Indeed, for $(a, b) = 1$:

$$(f \circ g(a)) \cdot (f \circ g(b)) = \left(\sum_{d_1 d_2 = a} f(d_1)g(d_2) \right) \left(\sum_{d_3 d_4 = b} f(d_3)g(d_4) \right) = \sum_{d_1 d_2 = a, d_3 d_4 = b} f(d_1 d_3)g(d_2 d_4) \tag{16}$$

Now we just need to convince ourselves that this is equivalent to $\sum_{u_1 u_2 = ab} f(u_1)g(u_2)$, but this is clear: since $(a, b) = 1$, if $u_1 u_2 = ab$, u_1 can be uniquely factored into $d_1 d_3$ such that $d_1 | a, d_3 | b$, and same for u_2.

Ex. 2.10 Show that $\phi(n) = n \sum_{d|n} \mu(d)/d$ by first proving that $\mu(d)/d$ is multiplicative and then using Ex. 2.9 and 2.10.

The function $\mu d/d$ is multiplicative, as it's a pointwise product of two multiplicative functions, $\mu(d)$ and $1/d$. Therefore, by Ex. 2.10, $\sum_{d|n} \mu d/d$ is also multiplicative, and so is $n \sum_{d|n} \mu d/d$, as a pointwise product of multiplicative functions (obviously n is multiplicative). Let $f(n) = n \sum_{d|n} \mu d/d$. As f is multiplicative, it is fully determined by its values on prime powers. If we show that $f(p^n) = \phi(p^n)$, it implies that $f = \phi$.

The only $1 \leqslant i \leqslant p^n$ that aren't relatively prime with p are multiples of p. These are $p, 2p, 3p, \ldots, p^{n-1}p^n$. There are exactly p^{n-1} elements on this list, so $\phi(p^n) = p^n - p^{n-1}$.

On the other hand, $f(p^n) = p^n \sum_{d|p^n} \mu(d)/d$. The only $d|p^n$ such that $\mu(d) \neq 0$ is $d = 1$ and $d = p$. Thus, $f(p^n) = p^n \sum_{d|p^n} \mu d/d = p^n(1 - 1/p)$, and so $f(p^n) = \phi(p^n)$.

Ex. 2.12 Find formulas for $f(n) = \sum_{d|n} \mu(d)\phi(d)$, $g(n) = \sum_{d|n} \mu(d)^2\phi(d)^2$, and $h(n) = \sum_{d|n} \mu(d)/\phi(d)$.

All of the functions are multiplicative, by Ex. 2.9. Let's determine their values on prime powers.

We have:

$$f(p^n) = \sum_{p^k | p^n} \mu(p^k)\phi(p^k) = \phi(1) - \phi(p) = -1 - p + 1 = -p \tag{17}$$

Thus $f(n) = (-1)^k \prod_{i=1}^k p_i$, where p_i are distinct prime factors of n.

$$g(p^n) = \sum_{p^k | p^n} \mu(p^k)^2\phi(p^k)^2 = \phi(1)^2 + \phi(p)^2 = 1 + p^2 - 2p + 1 = p^2 - 2p + 2 \tag{18}$$

Formula for $g(n)$ easily follows, but doesn't seem to be interesting.

$$f(p^n) = \sum_{p^k | p^n} \mu(p^k)/\phi(p^k) = 1/\phi(1) - 1/\phi(p) = -1 - \frac{1}{p-1} = \frac{-p}{p-1} \tag{19}$$

Ex. 2.13 Let $\sigma_k(n) = \sum_{d|n} d^k$. Show that $\sigma_k(n)$ is multiplicative and find a formula for it.

It is clearly multiplicative, since $f(n) = n^k$ is multiplicative. We have:

$$\sigma_k(p^n) = \sum_{d|p^n} d^k = 1 + p^k + (p^2)^k + \ldots + (p^n)^k = 1 + p^k + (p^k)^2 + \ldots + (p^k)^n = \frac{1 - (p^k)^{n+1}}{1 - p^k} \tag{20}$$

Ex. 2.14 If $f(n)$ is multiplicative, show that $h(n) = \sum_{d|n} \mu(n/d) f(d)$ is also multiplicative.

It follows from our solution to Ex. 2.9, as μ is multiplicative.

Ex. 2.15 Show that

a $\sum_{d|n} \mu(n/d)\nu(d) = 1$ for all n.

b $\sum_{d|n} \mu(n/d)\sigma(n) = n$ for all n.

Both of the left hand sides are multiplicative functions of n, so it's enough to determine their value on prime powers. We have:

$$\sum_{d|p^n} \mu(p^n/d)\nu(d) = \mu(p^n/p^{n-1})\nu(p^{n-1}) + \mu(p^n/p^n)\nu(p^n) = \mu(p)\nu(p^{n-1}) + \mu(1)\nu(p^n) = -n + n + 1 = 1 \tag{21}$$

since for d other than p^{n-1} and p^n, $\mu(p^n/d)$ is 0.

For (b),

$$\begin{aligned}
\sum_{d|p^n} \mu(p^n/d)\sigma(d) &= \mu(p^n/p^{n-1})\sigma(p^{n-1}) + \mu(p^n/p^n)\sigma(p^n) && (22)\\
&= \mu(p)\sigma(p^{n-1}) + \mu(1)\sigma(p^n) && (23)\\
&= -\frac{p^n - 1}{p - 1} + \frac{p^{n+1} - 1}{p - 1} && (24)\\
&= \frac{1 - p^n - 1 + p^{n+1}}{p - 1} = \frac{p^n(p - 1)}{p - 1} && (25)\\
&= p^n && (26)
\end{aligned}$$

Ex. 2.16 Show that $\nu(n)$ is odd iff n is a square.

This follows immediately from the formula:

$$\nu(\prod p_i^{a_i}) = \prod (a_i + 1) \tag{27}$$

Ex. 2.17 Show that $\sigma(n)$ is odd iff n is a square or twice a square.

We have:

$$\sigma(n) = \sigma(\prod p_i^{a_i}) = \prod_i \sum_{j=0}^{a_i} p^j \tag{28}$$

For $\sigma(n)$ to be odd, it is necessary and sufficient that each of the factors $\sum_{j=0}^{a_i} p^j$ is odd. For odd p, if a_i even, then $\sum_{j=0}^{a_i} p^j$ has odd number of odd summands, and therefore is odd. For $p = 2$, the sum is always odd. The thesis now follows.

Ex. 2.18 Prove that $\phi(n)\phi(m) = \phi((n, m))\phi([n, m])$.

We have:

$$\phi([n, m]) = \phi(nm/(n, m)) = \phi(n/(n, m))\phi(m) = \phi(n)\phi(m/(n, m)) \tag{29}$$

Now (n, m) must be relatively prime with one of $n/(n, m)$, $m/(n, m)$ – otherwise, if there was a prime divisor p of (n, m) that was also a prime divisor of both $n/(n, m), m/(n, m)$, it would mean that $p(n, m)$ divides both n and m, and so (n, m) would not be a greatest common divisor of n and m. Without loss of generality we can assume that (n, m) is relatively prime with $n/(n, m)$. Multiplying (29) by $\phi((n, m))$ we get:

$$\phi((n,m))\phi([n,m]) = \phi((n,m))\phi(n/(n,m))\phi(m) = \phi((n,m)\cdot n/(n,m))\phi(m) = \phi(n)\phi(m) \tag{30}$$

which is what we wanted to show.

Ex. 2.19 Prove that $\phi(nm)\phi((n,m)) = (n,m)\phi(n)\phi(m)$.

Ex. 2.20 Prove that $\prod_{d|n} d = n^{\nu(n)/2}$.

Ex. 2.21 Define $\wedge(n) = \log p$ if n is a power of p and zero otherwise. Prove that $\sum_{d|n} \mu(n/d)\log d = \wedge(n)$.

Let $f(n) = \sum_{d|n} \wedge(d)$. Clearly, this is the same as $f(n) = \sum_{p^k|n} \log p$, and there are exactly $ord_p n$ summands equal to $\log p$. Thus, $f(n) = \log \prod_{p^k|n} p = \log \prod_{p|n} p^{ord_p n} = \log n$. The equality now follows from Moebius inversion formula.

Ex. 2.22 Show that the sum of all the integers t such that $1 \leqslant t \leqslant n$ and $(t,n) = 1$ is $\frac{1}{2}n\phi(n)$.

Let $f(n)$ be the sum in question. Consider fractions $1/n, 2/n, \ldots, n/n$, and reduce them to lower terms. The possible denominators are all $d|n$. Consider the sum of numerators of fractions with denominators equal to d. These are all $1 \leqslant t \leqslant d$ with $(t,d) = 1$, and so the sum will be equal to $f(d)$. They all come from some fractions k/n by dividing the numerator and denominator by n/d, so the sum of all k-s in the fractions k/n that reduce to a fraction with denominator d will be exactly $n/df(d)$. Therefore, the following equality holds:

$$\sum_{d|n} \frac{n}{d} f(d) = \frac{n(n+1)}{2} \tag{31}$$

which is equivalent to:

$$\sum_{d|n} \frac{f(d)}{d} = \frac{n+1}{2} \tag{32}$$

We apply Moebius inversion formula:

$$\frac{f(n)}{n} = \sum_{d|n} \mu\left(\frac{n}{d}\right) \frac{d+1}{2} = \frac{1}{2}\left(\sum_{d|n} \mu\left(\frac{n}{d}\right) d + \sum_{d|n} \mu\left(\frac{n}{d}\right)\right) \tag{33}$$

The second sum is 0, so we are left with proving that $\sum_{d|n} \mu\left(\frac{n}{d}\right) d = \phi(n)$, but this follows instantly by applying Moebius inversion formula to the equality $n = \sum_{d|n} \phi(d)$.

Ex. 2.23 Let $f(x) \in \mathbb{Z}[x]$ and let $\psi(n)$ be the number of $f(j), j = 1, 2, \ldots, n$, such that $(f(j), n) = 1$. Show that $\psi(n)$ is multiplicative and that $\psi(p^t) = p^{t-1}\psi(p)$. Conclude that $\psi(n) = n\prod_{p|n} \psi(p)/p$.

Suppose a, b are relatively prime, and $1 \leqslant j \leqslant ab$. Then $f(j)$ is relatively prime to ab if and only if it is relatively prime to both a and b. Clearly, $f(j)$ is relatively prime to a iff $f(j) \mod a$ is relatively prime to a, but since f is polynomial, $f(j) \mod a = f(j \mod a)$. Since the same holds for b, $f(j)$ is relatively prime to ab if and only if $f(j \mod a)$ is relatively prime to a, and $f(j \mod b)$ is relatively prime to b. Since $f(0) = f(a) \mod a$, there are exactly $\psi(a)\psi(b)$ numbers $1 \leqslant j \leqslant ab$ such that $f(j)$ is relatively prime to ab – by the reasoning above, each such j gives us a pair $(j \mod a, j \mod b)$ (where mod are taken to be in $1, \ldots a$ and $1, \ldots, b$ instead of $0, \ldots, a-1$ and $0, \ldots, b-1$) such that $(f(j \mod a), a) = 1, (f(j \mod b), b) = 1$, and each pair $(r,s), 1 \leqslant r \leqslant a, 1 \leqslant s \leqslant b, (f(r), a) = 1, (f(s), b) = 1$ gives us by Chinese remainder theorem a number j in $1, \ldots, ab$ such that $(f(j), ab) = 1$.

Now let $n = p^t$. For $1 \leqslant j \leqslant p^t$ we have $(f(j), p^t) = (f(j), p) = (f(j) \mod p, p) = (f(j \mod p), p)$. Thus $(f(j), p^t) = 1$ iff $(f(j \mod p), p) = 1$. For $1 \leqslant j' \leqslant p$ there are exactly p^{t-1} different j, $1 \leqslant j \leqslant p^t$ such that $j \mod p = j'$. Thus, $\psi(p^t) = p^{t-1}\psi(p)$.

Now, since ψ is multiplicative, for $n = \prod_i p_i^{a_i}$ we have $\psi(n) = \psi(\prod_i p_i^{a_i}) = \prod_i \psi(p_i^{a_i}) = \prod_i p^{a_i-1}\psi(p) = \prod_i p^{a_i}\psi(p_i)/p_i = n\prod_i \psi(p_i)/p_i$.

Ex. 2.24 Supply the details to the proof of Theorem 3.

Since the Theorem 3 doesn't have any details left to supply, I assume that the author means Theorem 4 here:

Theorem 4. $\sum q^{-\deg p(x)}$ diverges, where the sum is over all monic irreducibles $p(x) \in k[x]$.

In the text authors show that $\sum q^{-\deg f(x)}$ diverges, and $\sum q^{-2\deg f(x)}$ converges, where the sum is taken over all monic polynomials. We now need to show that the same holds when one takes the sum over only irreducibles.

Let $p_1, p_2, \ldots, p_{l(n)}$ be all monic irreducible with degree no larger than n, and define:

$$\lambda(n) = \prod_{i=1}^{l(n)} \left(1 - q^{-\deg(p_i)}\right)^{-1} \tag{34}$$

Letting $l(n) = l$, we have:

$$\begin{aligned}
\lambda(n) &= \prod_{i=1}^{l} \sum_{j=0}^{\infty} q^{-a_j \deg(p_i)} = \prod_{i=1}^{l} \sum_{j=0}^{\infty} q^{-\deg(p_i^{a_j})} && (35)\\
&= \sum \left(q^{\deg(p_1^{a_1})} q^{\deg(p_2^{a_2})} \ldots q^{\deg\left(p_l^{a_l}\right)}\right)^{-1} && (36)\\
&= \sum \left(q^{\deg(p_1^{a_1}) + \deg(p_2^{a_2}) + \ldots + \deg\left(p_l^{a_l}\right)}\right)^{-1} && (37)\\
&= \sum \left(q^{\deg\left(p_1^{a_1} p_2^{a_2} \cdots p_l^{a_l}\right)}\right)^{-1} && (38)
\end{aligned}$$

where the sum is taken over all l-tuples of nonnegative integers $(a_1, \ldots, a_l)$. Clearly, every polynomial $f \in k[x]$ with $\deg(f) \leqslant n$ can be written as $f = p_1^{a_1} p_2^{a_2} \cdots p_l^{a_l}$ for some $a_1, \ldots, a_l$. Therefore $\lambda(n) > \sum_{\deg(f) \leqslant n} q^{-\deg(f)}$, and the latter sum diverges as $n \to \infty$, and so $\lambda(n) \to \infty$. Therefore there are infinitely many irreducible polynomials in $k[x]$.

Consider $\log \lambda(n)$. We have:

$$\begin{aligned}
\log \lambda(n) &= = -\sum_{i=1}^{l} \log\left(1 - q^{-\deg(p_i)}\right) = \sum_{i=1}^{l} \sum_{m=1}^{\infty} (m q^{m \deg(p_i)})^{-1} && (39)\\
&= q^{-\deg(p_1)} + q^{-\deg(p_2)} + \ldots + q^{-\deg(p_l)} + \sum_{i=1}^{l} \sum_{m=2}^{\infty} (m q^{m \deg(p_i)})^{-1} && (40)
\end{aligned}$$

Now, $\sum_{m=2}^{\infty} (m q^{m \deg(p_i)})^{-1} < \sum_{m=2}^{\infty} q^{-m \deg(p_i)} = q^{-2\deg(p_i)} (1 - q^{-\deg(p_i)})^{-1} \leqslant 2q^{-2\deg(p_i)}$. Therefore:

$$\begin{aligned}
\log \lambda(n) &= q^{-\deg(p_1)} + q^{-\deg(p_2)} + \ldots + q^{-\deg(p_l)} + \sum_{i=1}^{l} \sum_{m=2}^{\infty} (m q^{m \deg(p_i)})^{-1} && (41)\\
&\leqslant \sum_{i=0}^{\infty} q^{-\deg(p_i)} + \sum_{i=1}^{\infty} 2q^{-2\deg(p_i)} && (42)
\end{aligned}$$

We know that $\sum_{\deg(f) \leqslant n} q^{-2\deg(f)}$ converges, where the sum is taken over all monic f, so $\sum_{i=1}^{\infty} 2q^{-2\deg(p_i)}$ also converges. Therefore, if $\sum_{i=0}^{\infty} q^{-\deg(p_i)}$, $\log \lambda(n)$ would have been bounded, which is not true, since $\lambda(n)$ diverges.

Ex. 2.25 Consider the function $\zeta(s) = \sum_{n=1}^{\infty} 1/n^s$. ζ is called the Riemann zeta function. It converges for s ¿ 1. Prove the formal identity (Euler's identity) $\zeta(s) = \prod_p (1 - 1/p^s)^{-1}$.

We have:

$$\prod_p (1 - 1/p^s)^{-1} = \prod_p \sum_{i=0}^{\infty} \frac{1}{(p^i)^s} \tag{43}$$

For $n = \prod p_i^{a_i}$, $n^s = \prod (p_i^{a_i})^s$, so $1/n^s = 1/\prod (p_i^{a_i})^s$ is a summand of the product above.

Ex. 2.26 Verify the formal identities:

a) $\zeta(s)^{-1} = \sum \mu(n)/n^s$

We have:

$$\left(\sum \frac{\mu(n)}{n^s}\right) \cdot \zeta(s) = \sum_n \sum_{d|n} \frac{\mu(d)}{d^s(n/d)^s} = \sum_n \frac{1}{n^s} \sum_{d|n} \mu(d) = 1 \tag{44}$$

since $\sum_{d|n} \mu(d) = 0$ for $n \neq 1$.

b) $\zeta(s)^2 = \sum \nu(n)/n^s$

We have:

$$\zeta(s)^2 = \sum_n \sum_{d|n} \frac{1}{d^s(n/d)^s} = \sum_n \frac{1}{n^s} \sum_{d|n} 1 = \sum_n \frac{\nu(n)}{n^s} \tag{45}$$

c) $\zeta(s)\zeta(s-1) = \sum \sigma(n)/n^s$

We have:

$$\begin{aligned} \zeta(s)\zeta(s-1) &= \left(\sum_{n=1}^{\infty} 1/n^s\right)\left(\sum_{n=1}^{\infty} 1/n^{s-1}\right) && (46)\\ &= \left(\sum_{n=1}^{\infty} 1/n^s\right)\left(\sum_{n=1}^{\infty} n/n^s\right) && (47)\\ &= \sum_n \sum_{d|n} \frac{d}{(n/d)^s d^s} = \sum_n \frac{1}{n^s} \sum_{d|n} d = \sum_n \frac{\sigma(n)}{n^s} && (48) \end{aligned}$$

Ex. 2.27 Show that $\sum 1/n$, the sum being over square free integers, diverges. Conclude that $\prod_{p<N}(1+1/p) \to \infty$ as $N \to \infty$. Since $e^x > 1 + x$, conclude that $\sum_{p<N} 1/p \to \infty$.

Any nonnegative n can be written uniquely as $n = ab^2$, a square free. Thus, we have:

$$\sum_{n=1}^{\infty} \frac{1}{n} = \sum_{a \text{ square free}} \sum_{b=1}^{\infty} \frac{1}{ab^2} = \sum_{a \text{ square free}} \frac{1}{a} \sum_{b=1}^{\infty} \frac{1}{b^2} = \frac{\pi^2}{6} \sum_{a \text{ square free}} \frac{1}{a} \tag{49}$$

Thus, if $\sum_{a \text{ square free}} 1/a$ converged, so would $\sum_n 1/n$, which is known to diverge.

Therefore, we have:

$$\prod_{p<N} (1 + \frac{1}{p}) = \sum_a \frac{1}{a} \tag{50}$$

where sum is taken over all square free a such that their prime factos are smaller than N. Thus $\prod_{p<N}(1+\frac{1}{p}) \to \sum_{a \text{ square free}} 1/a = \infty$. But since $e^x > 1 + x$,

$$\prod_{p<N} (1 + \frac{1}{p}) \leqslant \prod_{p<N} e^{1/p} = e^{\sum_{p<N} 1/p} \tag{51}$$

If $\sum_p 1/p$ converged, $\prod_p(1 + \frac{1}{p})$ would have been bounded by $e^{\sum_p 1/p}$, but we have just shown it diverges.

3 Chapter 3

Ex. 3.1 Show that there are infinitely many primes congruent to -1 modulo 6.

All primes are congruent either to 1 or -1 modulo 6. Suppose $p_1, \ldots, p_n$ is a list of all primes congruent to -1 modulo 6. Consider a number $6p_1p_2 \cdots p_n - 1$. It is relatively prime to all of p_i, so all of its prime factors must be congruent to 1 modulo 6. But if it was the case, it would also have been congruent to 1 modulo 6, but we see that it is congruent to -1 modulo 6.

Ex. 3.2 Construct addition and multiplication tables for $\mathbb{Z}/5\mathbb{Z}, \mathbb{Z}/8\mathbb{Z}, and\mathbb{Z}/10\mathbb{Z}$.

Skipped.

Ex. 3.3 Let abc be the decimal representation for an integer between 1 and 1000. Show that abc is divisible by 3 iff $a+b+c$ is divisible by 3. Show that the same result is true if we replace 3 by 9. Show that abc is divisible by 11 iff $a-b+c$ is divisible by 11. Generalize to any number written in decimal notation.

Let $n = \sum_{i=0}^{k} a_i 10^i$ for $0 \leqslant a_i \leqslant 9$. Then n is divisible by 3 iff $n \equiv 0 \pmod 3$. But $10 \equiv 1 \mod 3$, so $n \equiv \sum_{i=0}^{k} a_i \pmod 3$. For divisibility by 9 and 11 note that $10 \equiv 1 \pmod 9$ and $10 \equiv -1 \pmod{11}$.

Ex. 3.4 Show that the equation $3x^2 + 2 = y^2$ has no solution in integers.

We have either $y^2 \equiv 0 \pmod 3$ or $y^2 \equiv 1 \pmod 3$, while the left hand side is congruent to 2 modulo 3.

Ex. 3.5 Show that the equation $7x^2 + 2 = y^3$ has no solution in integers.

The left hand side is congruent to 2 mod 7, while possible values of $y^3 \pmod 7$ are $0^3 = 0$, $1^3 = 1$, $2^3 = 8 \equiv 1 \pmod 7$, $3^3 = 27 \equiv 6 \pmod 7$, $4^3 = 16 \cdot 4 \equiv 2 \cdot 4 \equiv 1 \pmod 7$, $5^3 = 25 \cdot 5 \equiv 4 \cdot 5 \equiv 20 \equiv 6 \pmod 7$, and $6^3 = 36 \cdot 6 \equiv 1 \cdot 6 \equiv 6 \pmod 7$.

Ex. 3.6 Let an integer $n > 0$ be given. A set of integers $a_1, \ldots, a_{\phi(n)}$ is called a reduced residue system modulo n if they are pairwise incongruent modulo n and $(a_i, n) = 1$ for all i. If $(a, n) = 1$, prove that $aa_1, aa_2, \ldots, aa_{\phi(n)}$ is again a reduced residue system modulo n.

Let b be inverse to a modulo n, that is, $ab \equiv 1 \pmod n$ (it exists, because $(a, n) = 1 \pmod n$. Suppose $aa_i \equiv aa_j \pmod n$. Then $baa_i \equiv baa_j \pmod n$, so $a_i \equiv a_j \pmod n$, and so $i = j$, thus $aa_1, aa_2, \ldots, aa_{\phi(n)}$ are pairwise incongruent. As $(a, n) = 1$ and $(a_i, n) = 1$, we also have $(aa_i, n) = 1$ – otherwise, if aa_i and n had common prime factor, it would have to be one of the factors of a or a_i, but they have no common factors with n.

Ex. 3.7 Use Ex. 2.6 to give another proof of Euler's theorem, $a^{\phi(n)} \equiv 1 \pmod n$ for $(a, n) = 1$.

If $a_1, \ldots, a_{\phi(n)}$ and $b_1, \ldots, b_{\phi(n)}$ are two reduced residue systems modulo n, there exists a unique bijection f such that $a_i \equiv b_{f(i)} \pmod n$ for all i – to find it, note that $a_1 \mod n, \ldots, a_{\phi(n)} \mod n$ are all the different integers between 1 and n relatively prime to n, and same for b_i. Thus, we have:

$$\prod_{i=1}^{\phi(n)} a_i \equiv \prod_{i=1}^{\phi(n)} b_{f(i)} = \prod_{i=1}^{\phi(n)} b_i \pmod n \tag{52}$$

Now take $b_i = aa_i$. We have:

$$\prod_{i=1}^{\phi(n)} a_i \equiv \prod_{i=1}^{\phi(n)} aa_i = a^{\phi(n)} \prod_{i=1}^{\phi(n)} a_i \pmod n \tag{53}$$

Since all a_i are invertible modulo n, their product also is, so multiplying the equation above by the inverse of $\prod_{i=1}^{\phi(n)} a_i$ we get the desired equality.

Ex. 3.8 Let p be an odd prime. If $k \in \{1, 2, \ldots, p-1\}$, show that there is a unique b_k in this set such that $kb_k \equiv 1 \pmod p$. Show that $k \neq b_k$ unless $k = 1$ or $k = p - 1$.

The existence and uniqueness of b_k follow from the fact that $\mathbb{Z}/p\mathbb{Z}$ is a field. Now assume that $k^2 \equiv 1 \pmod p$, or equivalently $k^2 - 1 \equiv 0 \pmod p$. Then $(k-1)(k+1) \equiv 0 \pmod p$, but since $\mathbb{Z}/p\mathbb{Z}$ is an field, either $k - 1 \equiv 0 \pmod p$, or $k + 1 \equiv 0 \pmod p$. First case corresponds to $k = 1$, and the second to $k = p - 1$.

Ex. 3.9 Use Ex. 3.7 to prove that $(p-1)! \equiv -1 \pmod p$.

Of course, authors here mean Ex. 3.8, and the desired inequality follows immediately from it – since every k except of $k = p - 1$ is uniquely paired with corresponding b_k such that $kb_k \equiv 1 \pmod p$, we can group factors of $(p-1)!$ other than p-1 into pairs such that their product is congruent to 1 modulo p. Thus $(p-1)! \equiv p - 1 \equiv -1 \pmod p$.

Ex. 3.10 If n is not a prime, show that $(n-1)! \equiv 0 \pmod n$, except when $n = 4$.

If n is not a prime and not a square of a prime, it can be written as $n = ab$ with $1 < a < b < n$. Both a and b are factors of $(n-1)!$, but since $ab \equiv 0 \pmod n$, $(n-1)! \equiv 0 \pmod n$ also.

If n is a square of a prime, $n = p^2$, and $n \neq 4$, then $1 < p < 2p < p^2$, so both p and $2p$ are factors of $(p^2-1)!$, but $p \cdot 2p = 2p^2 \equiv 0 \pmod{p^2}$.

If $n = 4$, $(n-1)! = 2 \cdot 3 = 6 \equiv 2 \pmod 4$.

Ex. 3.11 Let $a_1, \ldots, a_{\phi(n)}$ be a reduced residue system modulo n and let N be the number of solutions to $x^2 \equiv 1 \pmod{n}$. Prove that $a_1 \cdots a_{\phi(n)} \equiv (-1)^{N/2} \pmod{n}$.

All of $a_1, \ldots, a_{\phi(n)}$ are invertible modulo n, and their inverse is also in this set. If $a_i^2 \equiv 1 \pmod{n}$, then also $(-a_i)^2 \equiv 1 \pmod{n}$, and moreover, a_i is not congruent to $-a_i$ modulo n – otherwise, if $a_i \equiv -a_i \pmod{n}$, we'd have $2a_i \equiv 0 \pmod{n}$, which cannot happen, since a_i is invertible modulo n. Therefore, a_i can be grouped into pairs – if $a_i^2 \equiv 1$, we group a_i with $-a_i$, and if $a_i^2 \not\equiv 1$, we group it with its inverse, which is also in the reduced residue system. Thus, we get $\phi(n)/2$ pairs. For pairs of the form $\{a_i, a_i^{-1}\}$ the product $a_i a_i^{-1}$ is congruent to 1 modulo n, and for pairs of the form $\{a_i, -a_i\}$ their product is congruent to -1 modulo n. There are exactly $N/2$ pairs of the second form, from which the desired congruence follows.

Ex. 3.12 Let $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ be a binomial coefficient, and suppose p is prime. If $1 \leqslant k \leqslant p-1$, show that p divides $\binom{p}{k}$. Deduce $(a+b)^p \equiv a^p + b^p \pmod{p}$.

The divisibility is clear: since $\binom{p}{k} = \frac{p!}{k!(p-k)!}$, p divides the numerator, but none of the factors in the denominator is divisible by p, as they all are integers smaller than p.

The desired congruence now follows from the application of the binomial theorem:

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} \equiv a^p + b^p \pmod{p} \tag{54}$$

The congruence holds, since $\binom{p}{k} a^k b^{p-k} \equiv 0 \pmod{p}$, for $1 \leqslant k \leqslant p-1$, since $\binom{p}{k}$ is then divisible by p.

Ex. 3.13 Use Ex. 3.12 to give another proof of Fermat's theorem, $a^{p-1} \equiv 1 \pmod{p}$ if p does not divide a.

As a is invertible modulo p, it is enough to prove that $a^p \equiv a \pmod{p}$. We proceed by induction on a. The case $a = 1$ is trivial. Assume that $(a-1)^p \equiv a - 1 \pmod{p}$. By Ex. 3.12 we have:

$$a^p = ((a-1)+1)^p \equiv (a-1)^p + 1 \equiv a - 1 + 1 = a \pmod{p} \tag{55}$$

Ex. 3.14 Let p and q be distinct odd primes such that $p-1$ divides $q-1$. If $(n, pq) = 1$, show that $n^{q-1} \equiv 1 \pmod{pq}$.

The congruence $n^{q-1} \equiv 1 \pmod{pq}$ is equivalent to $n^{q-1} - 1$ being divisible by pq, which in turns is equivalent to being divisible by both p and q, thus $n^{q-1} \equiv 1 \pmod{pq}$ iff both $n^{q-1} \equiv 1 \pmod{p}$ and $n^{q-1} \equiv 1 \pmod{q}$. The second congruence follows immediately from Euler's theorem, while the first congruence follows from the fact that $q - 1 = a(p-1)$ for some a, so since by Euler theorem $n^{p-1} \equiv 1 \pmod{p}$, $n^{q-1} = n^{a(p-1)} = (n^{p-1})^a \equiv 1^a = 1 \pmod{p}$.

Ex. 3.15 For any prime p show that the numerator of $1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{p} - 1$ is divisible by p.

The theorem as stated is clearly wrong, e.g. for $p = 2$, $1 + 1/2 - 1 = 1/2$, for $p = 3$ we have $1 + 1/2 + 1/3 - 1 = 5/6$. We'll show the opposite theorem, namely that the numerator is *not* divisible by p.

We have:

$$\frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{p} = \frac{p!/2 + p!/3 + \ldots + p!/p}{p!} \tag{56}$$

Note that $p!/k$ are integers, all of which are divisible by p, except of the last one, which is not. Thus, their sum will not be divisible by p.

Ex. 3.16 Use the proof of the Chinese Remainder Theorem to solve the system $x \equiv 1 \pmod{7}$, $x \equiv 4 \pmod{9}$, $x \equiv 3 \pmod{5}$.

Skipped.

Ex. 3.17 Let $f(x) \in \mathbb{Z}[x]$ and $n = p_1^{a_1} \cdots p_t^{a_t}$. Show that $f(x) \equiv 0 \pmod{n}$ has a solution iff $f(x) \equiv 0 \pmod{p_i^{a_i}}$ has a solution for $i = 1, \ldots, t$.

Follows from Ex. 3.13.

Ex. 3.18 For $f \in \mathbb{Z}[x]$, let N be the number of solutions to $f(x) \equiv 0 \pmod{n}$ and N_i be the number of solutions to $f(x) \equiv 0 \pmod{p_i^{a_i}}$. Prove that $N = \prod N_i$.

Let $(b_1, \ldots, b_t)$ be a solution to a system $f(x) \equiv 0 \pmod{p_i^{a_i}}$. By Chinese remainder theorem there exists x such that $x \equiv b_i \pmod{p_i^{a_i}}$. We claim that x is a solution to $f(x) \equiv 0 \pmod{n}$. Indeed, this is the same as saying that $f(x)$ is divisible by $p_i^{a_i}$ for $i = 1, \ldots, t$. But since $x \equiv b_i \pmod{p_i^{a_i}}$, and f is a polynomial, $f(x) \equiv f(b_i) \equiv 0 \pmod{p_i^{a_i}}$, so $f(x)$ is divisible by $p_i^{a_i}$ for all i.

Thus, there's a one-to-one correspondence between tuples $(b_1, \ldots, b_t)$ forming solutions to $f(x) \equiv 0 \pmod{p_i^{a_i}}$, and x-s being the solutions to $f(x) \equiv 0 \pmod{n}$.

Ex. 3.19 If p is an odd prime, show that 1 and -1 are the only solutions to $x^2 \equiv 1 \pmod{p^a}$.

The given equation is equivalent to asking for $1 < x < p^a - 1$ such that $x^2 - 1$ is divisible by p^a. Now $x^2 - 1 = (x-1)(x+1)$, and since $p > 2$, if one factor is divisible by p, the other factor isn't, so the only way $(x-1)(x+1)$ is divisible by p^a is that either p^a divides $x-1$, or it divides $x+1$. As $1 < x < p^a - 1$, this is impossible.

Ex. 3.20 Show that $x^2 \equiv 1 \pmod{2^b}$ has one solution if $b = 1$, two solutions if $b = 2$, and four solutions if $b \geqslant 3$.

The cases $b = 1$ and $b = 2$ are trivial, so assume that $b \geqslant 3$. We ask for $1 \leqslant x \leqslant 2^b - 1$ such that $(x-1)(x+1)$ is divisible by 2^b, which is the same as asking that $ord_2(x-1)(x+1) = b$. We have $(x-1, x+1) = 2$, so necessarily $ord_2(x-1)(x+1) \leqslant \max(ord_2(x-1), ord_2(x+1)) + 1$. For $1 < x < 2^b - 1$, $\max(ord_2(x-1), ord_2(x+1)) + 1 < b$ except for x such that $x - 1 = 2^{b-1}$ or $x + 1 = 2^{b-1}$. These are 2 solutions, and since $b > 3$, they aren't equal to $x = 1$ or $x = -1$.

Ex. 3.21 Use Ex. 3.18-3.20 to find the number of solutions to $x^2 \equiv 1 \pmod{n}$.

Write $n = 2^a p_1^{a_1} \cdots p_t^{a_t}$ for $p_1 \neq 2$. By Ex. 3.18, the number of solutions is equal the number of solutions modulo 2^a times the numbers of solutions modulo $p_i^{a_i}$. By Ex. 3.19 and 3.20, this is equal to 2^t for $a = 0, 1$, 2^{t+1} for $a = 2$ and 2^{t+2} for $a \geqslant 3$.

Ex. 3.22 Formulate and prove the Chinese Remainder Theorem in a principal ideal domain.

Let A be a PID. Let $m_1, \ldots, m_n$ be such that $(m_i, m_j) = A$. Then $A/(m_1 \cdots m_n) \simeq A/(m_1) \times \cdots \times A/(m_n)$.

The proof is omitted, as it is exactly the same as proof for $\mathbb{Z}$.

Ex. 3.23 Extend the notion of congruence to the ring $\mathbb{Z}[i]$ and prove that $a + bi$ is always congruent to 0 or 1 modulo $1 + i$.

Let π be a prime element of $\mathbb{Z}[i]$. Then for $x, y \in \mathbb{Z}[i]$, x is said to be congruent modulo π iff $x - y$ is divisible by π.

Note that $(1+i)^2 = 1 + 2i - i^2 = 2i$, so $2i \equiv 0 \pmod{1+i}$. Now take any $a + bi \in \mathbb{Z}[i]$. If $a - b$ is even, then:

$$a + bi \equiv a + bi + \frac{a-b}{2} \cdot 2i \equiv a + ai \equiv a(1+i) \equiv 0 \pmod{1+i} \tag{57}$$

Alternatively, if $a - b$ is odd, then $a - 1 + bi \equiv 0 \pmod{1+i}$ by the reasoning above, so $a - 1 + bi \equiv 0 \pmod{1+i}$, and so $a + bi \equiv 1 \pmod{1+i}$.

Ex. 3.24 Extend the notion of congruence to the ring $\mathbb{Z}[\omega]$ and prove that $a + b\omega$ is always congruent to -1, 0 or 1 modulo $1 - \omega$.

Note that $(1-\omega)(1+\omega)(1-\omega) = (1-\omega^2)(1-\omega) = (1-\bar{\omega})(1-\omega) = 1 - \omega - \bar{\omega} + \omega\bar{\omega} = 1 - (2\Re\omega) + |\omega|^2 = 1 + 1 + 1 = 3$. Reasoning now is similar to the reasoning in Ex. 3.23.

Ex. 3.25 Let $\lambda = 1 - \omega \in \mathbb{Z}[\omega]$. If $\alpha \in \mathbb{Z}[\omega]$ and $\alpha \equiv 1 \pmod{\lambda}$, prove that $\alpha^3 \equiv 1 \pmod{9}$.

If $\alpha \equiv 1 \pmod{\lambda}$, then $\alpha = 1 + \beta\lambda$, for some $\beta \in \mathbb{Z}[\omega]$. Then $\alpha^3 = 1 + 3\beta\lambda + 3\beta^2\lambda^2 + \beta^3\lambda^3$. Substituting $\lambda = 1 - \omega$, we get:

$$\begin{aligned}
\alpha^3 - 1 &= 3\beta\lambda + 3\beta^2\lambda^2 + \beta^3\lambda^3 && (58)\\
&= 3\beta - 3\beta\omega + 3\beta^2 - 6\beta^2\omega + 3\beta^2\omega^2 - 3\beta^3\omega + 3\beta^3\omega^2 && (59)\\
&= 3\beta(1 - \omega + \beta - 2\beta\omega + \beta\omega^2 - \beta^2\omega + \beta^2\omega^2) && (60)\\
&= 3\beta(1 - 2\beta\omega + \beta^2\omega^2 - \omega + \beta\omega^2 + \beta - \beta^2\omega) && (61)\\
&= 3\beta((1 - \beta\omega)^2 - \omega(1 - \beta\omega) + \beta(1 - \beta\omega)) && (62)\\
&= 3\beta(1 - \beta\omega)(1 - \beta\omega - \omega + \beta) && (63)\\
&= 3\beta(1 - \beta\omega)(1 + \beta)(1 - \omega) && (64)
\end{aligned}$$

It is now enough to show that $\beta(1 - \beta\omega)(1 + \beta)(1 - \omega)$ is divisible by 3, so we can work modulo 3. We let $\beta = a + b\omega$, and after reducing modulo 3 we can assume that $-1 \leqslant a, b \leqslant 1$. We have:

$$\begin{aligned}
\beta(1 - \beta\omega)(1 + \beta)(1 - \omega) &= 3(a + b\omega)(1 - (a + b\omega)\omega)(1 + a + b\omega)(1 - \omega) && (65)\\
&= (a + b\omega)(1 - a\omega - b\omega^2)(1 + a + b\omega)(1 - \omega) && (66)\\
&= (a + b\omega)(1 + b + (b - a)\omega)(1 + a + b\omega)(1 - \omega) && (67)
\end{aligned}$$

We need to prove that the expression above is divisible by 3. If $a = b = 0$, it is trivial so we can assume that at least one of a, b is nonzero. Note that $-\omega^2(1 - \omega)^2 = -\omega^2(1 - 2\omega + \omega^2) = -\omega^2 + 2 - \omega = 3 - 1 - \omega - \omega^2 = 3$, so $(1 - \omega)^2$ is divisible by 3.

If $a = 1, b = -1$, $a + b\omega = 1 - \omega$, so we get two factors of $1 - \omega$ in (65). If $a = 1, b = 0$, then $(1 + b + (b - a)\omega) = 1 - \omega$. If $a = 1, b = 1$, then $(1 + a + b\omega) = 2 + \omega$ (note that this is the same case as $-1 + \omega$). We can multiply it by ω (which is invertible) to get $\omega(2 + \omega) = 2\omega + \omega^2 = 2 - 1 - \omega = 1 - \omega$.

If $a = -1$, $b = -1$, then $1 + b + (b - a)\omega = 0$, and so the whole expression is 0, which is divisible by 3. If $a = -1, b = 0$, then $1 + b + (b - a)\omega = 1 - \omega$. The case $a = -1, b = 1$ has been dealt with above.

In all cases, we get the expression to equal 0, to have factor of $(1 - \omega)^2$, or to have a factor associated to $(1 - \omega)^2$ through multiplication by ω, and so we are done.

This seems to be like a very brute force approach to the problem above, and so I'm looking for a cleaner approach.

Ex. 3.26 Use Ex. 3.25 to show that ξ, η, ζ are not zero and $\xi^3 + \eta^3 + \zeta^3 = 0$, then λ divides at least one of the elements ξ, η, ζ.

Assume that λ divides none of ξ, η, ζ. We aim to show contradiction. By Ex. 3.24 we know that each of ξ, η, ζ must be congruent to -1 or 1 modulo λ. Clearly $\alpha^3 \equiv \alpha \pmod{\lambda}$ for any α, so since $\xi^3 + \eta^3 + \zeta^3 = 0$, and since $-1, 0, 1$ are different classes modulo λ, necessarily we have $\xi \equiv \eta \equiv \zeta \equiv \pm 1 \pmod{\lambda}$. Multiplying by -1, which is invertible, we can assume that they all are congruent to 1 modulo λ. Then, Ex. 3.25 tells us that $\xi^3 + \eta^3 + \zeta^3 \equiv 3 \pmod 9$, but $\xi^3 + \eta^3 + \zeta^3 = 0$ and $0 \not\equiv 3 \pmod 9$, which is a contradiction.

4 Chapter 4

Ex. 4.1 Show that 2 is a primitive root modulo 29.

We are asked to show that 2 generates the multiplicative group of the field $\mathbb{Z}/29\mathbb{Z}$, which has order 28. Since $28 = 4 \cdot 7$, it's enough that we show that its orderd is not either 2, 4, 7 or 14.

Note that $2^2 \equiv 4 \pmod{29}$, $2^4 \equiv 16 \pmod{29}$, $2^7 \equiv 4 \cdot 2^5 \equiv 4 \cdot 32 \equiv 4 \cdot 3 \equiv 12 \pmod{29}$, and $2^{14} \equiv (2^7)^2 \equiv 12^2 \equiv 144 \equiv 28 \pmod{29}$.

Ex. 4.2 Compute all primitive roots for $p = 11, 13, 17$, and 19.

Skipped.

Ex. 4.3 Suppose that a is a primitive root modulo p^n, p an odd prime. Show that a is a primitive root modulo p.

Assume that a is not a primitive root modulo p, that is, $a^k \equiv 1 \pmod p$ for some $k | p - 1$, $k < p - 1$. By repeated application of Lemma 3, from $a^k \equiv 1 \pmod p$ we get $(a^k)^{p^{n-1}} \equiv 1^{p^{n-1}} \pmod{p^n}$, so order of a is no larger than kp^{n-1}, which is smaller than $\phi(p^n) = p^{n-1}(p - 1)$. Therefore, a cannot be a primitive root modulo p^n.

Ex. 4.4 Consider a prime p of the form $4t+1$. Show that a is a primitive root modulo p iff $-a$ is a primitive root modulo p.

Assume that a is a primitive root modulo p. Suppose k is a smallest integer such that $(-a)^k \equiv 1 \pmod{p}$. We need to show that $k = p-1$. Note that $(-a)^k \equiv (-1)^k a^k \equiv 1 \pmod{p}$, and since a is a primitive root modulo p, if $k < p-1$, then also $a^k \not\equiv 1$, so we must have $(-1)^k \equiv -1 \pmod{p}$, that is, k is odd. Since $p = 4t+1$, $p-1$ is divisible by 4, and so $2k < p-1$. But then $a^{2k} = (-1)^{2k} a^{2k} = (-a)^{2k} = ((-a)^k)^2 \equiv 1^2 \pmod{p}$, and so a is not a primitive root modulo p.

Ex. 4.5 Consider a prime p of the form $4t+3$. Show that a is a primitive root modulo p iff $-a$ has order $(p-1)/2$.

Assume that a is a primitive root modulo p. Let k be the order of $-a$ modulo p. Now if $k < (p-1)/2$, reasoning as above, we conclude that k must be odd. Also $2k < p-1$, and reasoning as above, a is not a primitive root modulo p. Therefore, we get $k \geqslant (p-1)/2$.

On the other hand, if $-a$ had order strictly larger than $(p-1)/2$, the only remaining option is $p-1$, that is, $-a$ is a primitive root modulo p. It means that $(-a)^{(p-1)/2} \not\equiv 1 \pmod{p}$. But $(p-1)/2 = 2t+1$, so $(-1)^{2t+1} a^{2t+1} \not\equiv 1 \pmod{p}$, that is, $-a^{2t+1} \not\equiv 1 \pmod{p}$. But $(a^{2t+1})^2 = a^{p-1} \equiv 1 \pmod{p}$, and so since we are working in a field, a^{2t+1} is congruent to 1 or -1 modulo p. Since a is primitive root modulo p, it must be congruent to -1 modulo p, but then $-a^{2t+1} \equiv 1 \pmod{p}$, which is a contradiction.

In the other direction, assume tha $-a$ has order $(p-1)/2$. It means that $(-a)^{2t+1} \equiv 1 \pmod{p}$, that is, $a^{2t+1} \equiv -1 \pmod{p}$. Order of a modulo p must divide $p-1$, and the congruence above show that it does not divide $2t+1 = (p-1)/2$, so it must be equal to $p-1$.

Ex. 4.6 If $p = 2^{2^n}+1$ is a Fermat prime, show that 3 is a primitive root modulo p.

If the order of 3 is smaller than $p-1$, it must divide $(p-1)/2$, so it is enough to show that $3^{(p-1)/2} \equiv -1 \pmod{p}$, which is equivalent to saying that 3 is not a square modulo p. Since -1 is a square modulo p (as can be seen by Wilson theorem for any $p = 4t+1$), it follows that -3 is a non-square too, so it is enough to show that -3 cannot be square modulo p. Suppose it is, that is, $x^2 \equiv -3 \pmod{p}$ for some x. We can assume that x is odd – if $x = 2y$ and $(2y)^2 \equiv -3 \pmod{p}$, then we just replace $2y$ with $2y+p$, which is odd. Thus, $x = 2y+1$ for some y. Then if $(2y+1)^2 \equiv -3 \pmod{p}$, then $4y^2+4y+4 \equiv 0 \pmod{p}$, but 4 is invertible modulo p, so $y^2+y+1 \equiv 0 \pmod{p}$. It follows that $y^3 \equiv 1 \pmod{p}$, but since order of y must divide $p-1 = 2^n$, $y \equiv 1 \pmod{p}$. Thus $3^2 \equiv -3 \pmod{p}$, that is, $12 \equiv 0 \pmod{p}$, and since $12 = 2 \cdot 2 \cdot 3$, one of 2 of 3 is congruent to 0 modulo p, which is only true if $p = 3$ (since p is a Fermat prime). But $p \neq 3$ is a hidden assumption in th exercise, since in that case 3 clearly cannot be a primitive root modulo 3.

Ex. 4.7 Suppose that p is a prime of the form $8t+3$ and that $q = (p-1)/2$ is also a prime. Show that 2 is a primitive root modulo p.

By Ex. 4.5, it is enough to show that -2 has order $(p-1)/2 = q$. Let k be the order of -2. Since k must divide $p-1$, and $p-1 = 2q$, so k must be 2, q, or $2q$.

If the order is 2, then $(-2)^2 \equiv 1 \pmod{p}$, so $3 \equiv 0 \pmod{p}$, and so $p = 3$, but then $q = (p-1)/q$ is not prime.

If the order of -2 is $2q$, then -2 is a quadratic nonresidue. As $p = 8t+3$, -1 is also a quadratic nonresidue. Therefore 2 is a quadratic residue modulo p, but this is only true for p of the form $8t+1$, $8t+7$ (proved in the next chapter), which is a contradiction.

Ex. 4.8 Let p be an odd prime. Show that a is a primitive root modulo p iff $a^{(p-1)/q} \not\equiv 1 \pmod{p}$ for all prime divisors q of $p-1$.

One direction is clear: if $a^{(p-1)/q} \equiv 1 \pmod{p}$ for some q, then the order of a is smaller than $p-1$.

In the other direction, assume that the order of a is smaller than $p-1$, say $a^k \equiv 1 \pmod{p}$ for some $k < p-1$. The order k must divide $p-1$, so write $p-1 = kt$ for some $t > 1$. Let q be a prime divisor of t, so that $p-1 = kt'q$ for some t'. Then:

$$a^{(p-1)/q} \equiv a^{kt'} \equiv (a^k)^{t'} \equiv 1^{t'} \equiv 1 \pmod{p} \tag{68}$$

Ex. 4.9 Show that the product of all the primitive roots modulo p is congruent to $(-1)^{\phi(p-1)}$ modulo p.

Let g be any primitive root modulo p, and $\{a_1, \ldots, a_{\phi(p-1)}\}$ be a list of all positive integers smaller than $p-1$ and relatively prime to $p-1$. It follows that g^{a_i} are all distinct primitive roots modulo p. Their product is precisely $g^{\sum a_i}$. We will therefore investigate $\sum a_i$.

Note that if k is relatively prime to $p-1$, so is $p-1-k$. $k \neq p-1-k$, unless $2k = p-1$, but the only way a number k such that $2k = p-1$ is relatively prime to $p-1$ is when $k = 1$, $p-1 = 2$, and $p = 3$. We treat this case separately. Assume therefore that $p \neq 3$. We can divide numbers less than $p-1$ and relatively prime to $p-1$ into $\phi(p-1)/2$ pairs, the sum of numbers in each pair is equal to $p-1$. Therefore, the sum of all numbers smaller than $p-1$ and relatively prime to $p-1$ is exactly $(p-1)\phi(p-1)/2$.

Now, $g^{(p-1)\phi(p-1)/2} = (g^{(p-1)/2})^{\phi(p-1)}$. We have $g^{(p-1)/2} \equiv -1 \pmod{p}$, and so the desired congruence follows.

For $p = 3$, there's only one primitve root modulo 3, which is $2 =\equiv -1 \pmod{3}$. On the other hand $(-1)^{\phi(p-1)} = (-1)^{\phi(2)} = -1 \pmod{3}$.

Ex. 4.10 Show that the sum of all the primitive roots modulo p is congruent to $\mu(p-1)$ modulo p.

For any divisor k of $p-1$, let $\psi(k)$ denote the sum of elements of order k modulo p. We'll show that $\psi(k) = \mu(k)$, which implies the desired congruence.

First note that ψ is multiplicative modulo p.

If m, n are relatively prime, then $\mathbb{Z}/(mn) \simeq \mathbb{Z}/(m) \times \mathbb{Z}/(n)$ through isomorphism $a \mapsto (a \mod m, a \mod n)$ (Chinese remainder theorem). From this isomorphism it follows that every c of the order mn can be uniquely written as a product $c = ab$, with a having order m, and b order n.

Let $a_1, \ldots, a_s$ be all elements of $U(\mathbb{Z}/p\mathbb{Z})$ of order m, and $b_1, \ldots, b_t$ be all elements of $U(\mathbb{Z}/p\mathbb{Z})$ of order n. Since a_i and b_j are all elements of a cyclic subgroup C_{mn} of $U(\mathbb{Z}/p\mathbb{Z})$ of elements of orders dividing mn, the above reasoning applies. Therefore:

$$\psi(m)\psi(n) = (a_1 + \ldots + a_s)(b_1 + \ldots + b_t) = \sum_{1 \leqslant i \leqslant s} \sum_{1 \leqslant j \leqslant t} a_i b_j \equiv \psi(mn) \pmod{p} \tag{69}$$

We now show that $\psi(p^n) \equiv \mu(p^n) \pmod{p}$, which along with multiplicativity gives us desired conclusion.

We proceed by induction. For $n = 0$, the only element of order $p^0 = 1$ is 1, and its sum is $1 = \mu(1)$.

For $n > 0$, the sum of all elements of order p^n is the sum of all roots of $x^{p^n} \equiv 1 \pmod{p}$ minus the roots of $x^{p^{n-1}} \equiv 1 \pmod{p}$. Both of these sums are equal to 0 except in case when $p^{n-1} = 1$, that is, $n = 1$. In that case, there is only one root, 1, so $\psi(p) = -1$, and $\psi(p^n) = 0$ for $n > 1$.

Ex. 4.11 Prove that $1^k + 2^k + ... + (p-1)^k \equiv 0 \pmod{p}$ if $p-1 \not| k$, and $\equiv -1 \pmod{p}$ if $p-1 | k$.

If g is a primitive root, then $g, g^2, \ldots, g^{p-1}$ is a permutation of $1, 2, \ldots, p-1$ modulo p. Therefore:

$$1^k + 2^k + ... + (p-1)^k \equiv g^k + (g^2)^k + \ldots + (g^{p-1})^k \equiv g^k + (g^k)^2 + \ldots + (g^k)^{p-1} \pmod{p} \tag{70}$$

If $p-1|k$, $x^k = 1$, and so $1 + 1^2 + \ldots + 1^{p-1} = p-1 \equiv -1 \pmod{p}$. On the other hand, if $p-1 \not| k$, then $g^k \neq 1$. Write $x = g^k$. We want to show that $x + x^2 + \ldots + x^{p-1} \equiv 0 \pmod{p}$. We have:

$$x + x^2 + \ldots + x^{p-1} = x(1 + x + \ldots + x^{p-2}) \equiv x(x^{p-1} - 1)(x-1)^{-1} \equiv 0 \pmod{p} \tag{71}$$

since $x^{p-1} - 1 \equiv 0 \pmod{p}$.

Ex. 4.12 Use the existence of a primitive root to give another proof of Wilson's theorem $(p-1)! \equiv -1 \pmod{p}$.

If g is a primitive root, then $g, g^2, \ldots, g^{p-1}$ is a permutation of $1, 2, \ldots, p-1$ modulo p. Therefore:

$$(p-1)! \equiv g^1 \cdot g^{p-1} \equiv g^{1+2+\ldots+p-1} \equiv g^{p(p-1)/2} \equiv (g^p)^{(p-1)/2} \equiv g^{(p-1)/2} \equiv -1 \pmod{p} \tag{72}$$

Ex. 4.13 Let G be a finite cyclic group and $g \in G$ a generator. Show that all the other generators are of the form g^k, where $(k, n) = 1$, n being the order of G.

If $(k, n) = d \neq 1$, then $n | \frac{kn}{d}$, and so $(g^k)^{n/d} = g^{kn/d} = 1$. Thus the order of g^k divides n/d, which implies that it's smaller than n, and so g^k cannot generate G.

On the other hand, if $(k, n) = 1$, let $ak + bn = 1$. Then $g = g^{ak+bn} = g^{ak} g^{bn} = (g^k)^a (g^n)^b = (g^k)^a 1^b = (g^k)^a$. Thus g^k generates g, and so generates the whole group.

Ex. 4.14 Let A be a finite abelian group and $a, b \in A$ elements of order m and n, respectively. If $(m, n) = 1$, prove that ab has order mn.

Let M and N be subgroups generated by m and n respectively. Consider $a \in M \cap N$. Its order d must divide the order of M and the order of N, but since $(m, n) = 1$, we necessarily have that $d = 1$, and so $M \cap N = \{1\}$.

Note that $(ab)^{mn} = (a^m)^n (b^n)^m = 1$, so the order of ab must divide mn. Now, let e be the order of ab, that is, $(ab)^e = 1$. Then $a^e b^e = 1$. and so $a^e = b^{-e}$. It follows that $a^e \in B$, and $b^e \in A$, so $a^e = b^e = 1$. Thus, $m|e$ and $n|e$, and so e is a multiple of both m and n. Since $(m, n) = 1$, their smallest multiple is mn, and since we know that the order must divide mn, we get that the order is indeed mn.

Ex. 4.15 Let K be a field and $G \subset K^*$ a finite subgroup of the multiplicative group of K. Extend the arguments used in the proof of Theorem 1 to show that G is cyclic.

Let $n = |G|$. If K has characteristic 0, consider an extension $\mathbb{Q} \subset \mathbb{Q}(G)$. We say this is an algebraic extension: indeed, every element of G is a root of polynomial $x^n - 1$. Thus we can embed $\mathbb{Q}(G)$ in $\mathbb{C}$. In this embedding, G is a subgroup of the group of roots of $x^n - 1$. But in $\mathbb{C}$, this group has exactly n elements, and is cyclic, generated by $e^{2i\pi/n}$. Thus, G is a subgroup of a cyclic group, and so is cyclic itself.

If K has characteristic p, consider an extension $\mathbb{F}_p(G)$. Arguing as before, we say that this is an algebraic extension, but more importantly, it is also a finite extension, so $\mathbb{F}_p(G)$ is a finite field with p^k elements, for some k. In this embedding, G is a subgroup of the multiplicative group of $\mathbb{F}_{p^k}$. We now need to show that this group is cyclic.

The polynomial $x^{p^k-1} - 1$ has exactly $p^k - 1$ roots in $\mathbb{F}_{p^k}$. We now argue just like in proof of the Theorem 1 – if $d|p^k - 1$, then $x^d - 1 = 0$ has exactly d solutions in $\mathcal{F}_{p^k}$. Indeed, just like in Proposition 4.1.2, we prove that we have:

$$x^{p^k-1} - 1 = (x^d - 1)g(x) \tag{73}$$

for some (easy to calculate) polynomial $g(x)$. If $x^d - 1$ had less than d roots, then $x^{p^k-1} - 1$ necessarily would have less than $p^k - 1$ roots as well, but it contradicts the fact that all nonzero elements of $\mathcal{F}_{p^k}$ are roots of that polynomial, and there are $p^k - 1$ of them.

So, we continue just like in the proof of Theorem 1: we let $\psi(d)$ equal number of elements of $U(\mathcal{F}_{p^k})$ of order d, using reasoning above we conclude that $d = \sum_{c|d} \psi c$, we use Moebius inversion to conclude that $\psi(d) = \phi(d)$, and note that $\phi(p^k - 1) > 1$, so there exists an element of order $p^k - 1$.

Ex. 4.16 Calculate the solutions to $x^3 \equiv 1 \pmod{19}$ and $x^4 \equiv 1 \pmod{17}$.

Note that $x^3 - 1 = (x - 1)(x^2 + x + 1)$. We complete the square in $x^2 + x + 1$: the discriminant is $1 - 4 = -3 \equiv 16 \pmod{19}$, and so its square root is $4 \pmod{19}$. The inverse of 2 modulo 19 is 10, as $2 \cdot 10 = 20 \equiv 1 \pmod{19}$. Thus:

$$x^2 + x + 1 = (x - 2^{-1} \cdot (-1 - 4))(x - 2^{-1} \cdot (-1 + 4)) = (x - 10 \cdot 14)(x - 10 \cdot 3) = (x - 7)(x - 11) \tag{74}$$

We deal with the second equation in a similar manner: $x^4 - 1 = (x^2 - 1)(x^2 + 1) = (x - 1)(x + 1)(x^2 + 1)$, so it remains to find square roots of $-1 \equiv 16 \pmod{17}$, but these are just 4 and $-4 \equiv 13 \pmod{17}$.

Ex. 4.17 Use the fact that 2 is a primitive root modulo 29 to find the seven solutions to $x^7 \equiv 1 \pmod{29}$.

We can write $x \equiv 2^k \pmod{29}$ for some $k \in \{0, 1, \ldots, 27\}$. For $(2^k)^7 \equiv 1 \pmod{29}$ to be true, $7k$ must be a multiple of 28. This means that $k \in \{0, 4, 8, 12, 16, 20, 24\}$, and corresponding values of x are $1, 16, 24, 7, 25, 23, 20 \pmod{29}$.

Ex. 4.18 Solve the congruence $1 + x + \ldots + x^6 \equiv 0 \pmod{29}$.

Note that $(1 - x)(1 + x + \ldots + x^6) = 1 - x^7$. From the previous exercise we can find the roots to the right hand side, and except of $x = 1$, the remainding 6 solutions must be the solutions to $1 + x + \ldots + x^6 \pmod{29}$.

Ex. 4.19 Determine the numbers a such that $x^3 \equiv a \pmod{p}$ is solvable for $p = 7, 11, 13$.

This tedious exercise can be easily solved by a brute-force search, so I'll skip it.

Ex. 4.20 Let p be a prime, and d a divisor of $p-1$. Show that dth powers form a subgroup of $U(\mathcal{F}_p)$ of order $(p-1)/d$. Calculate this subgroup for $p=11, d=5$, for $p=17, d=4$, and for $p=19, d=6$.

Let $a=x^d, b=y^d$. Then obviously $ab=(xy)^d$, so ab is dth power. Similarly, $a^{-1}=(x^{-1})^d$, so a^{-1} is also dth power. Thus we see that dth powers form a subgroup.

If $x=y^d$ for some y, then $x^{(p-1)/d}-1=(y^d)^{(p-1)/d}-1=y^{p-1}-1=1-1=0$, so there are at most $(p-1)/d$ dth powers. Consider a function $f: U(\mathcal{F}_p)\to U(\mathcal{F}_p), f(a)=a^d$. The image has at most $(p-1)/d$ elements. Each element b in the image has at most d elements in the preimage, as they all must be solutions to $x^d=b$. If the image had strictly less than $(p-1)/d$ elements, the preimage of the image, which is $U(\mathcal{F}_p)$, would need to have strictly less than $d\cdot(p-1)/d=p-1$ elements, which is a contradiction.

For $p=11$, the subgroup of 5th powers have only $(11-10)/5=2$ elements. One of them is obviously 1, the other is e.g. $2^5=32\equiv -1=10 \pmod{11}$.

For $p=17$, the group of 4th elements has $(17-1)/4=4$ elements. These are 1, $2^4=16\equiv -1 \pmod{17}$, $3^4=81\equiv 13 \pmod{17}$, and $-13\equiv 4 \pmod{17}$.

For $p=19$, the subgroup of 6th power has 3 elements, which are 1, $2^6=64\equiv 7 \pmod{19}$, and $7^2=49\equiv 11 \pmod{19}$.

Ex. 4.21 If g is a primitive root modulo p, and $d|p-1$, show that $g^{(p-1)/d}$ has order d. Show also that a is a dth power iff $a\equiv g^{kd} \pmod{p}$ for some k. Do Exercises 4.16-4.20 making use those observations.

These observations are trivial, and we already used them above.

Ex. 4.22 If a has order 3 modulo p, show that $1+a$ has order 6.

We need to show that $(1+a)^k$ is not equal to 1 for $k<6$, and that $(1+a)^6=1$.

Note that as a has order 3 modulo p, we have:

$$0=a^3-1=(a-1)(1+a+a^2) \tag{75}$$

As a has order 3, $a\neq 1$, so $1+a+a^2=0$.

Now, let us handle all cases separately.

$k=1$: Since a has order 3, $a\neq 0$, and so $(1+a)^1\neq 1$.

$k=2$: We have $(1+a)^2=1+2a+a^2=1+a+a^2+a=a$. We know that $a\neq 1$.

$k=3$: We have $(1+a)^3=1+3a+3a^2+a^3=3(1+a+a^2)-1=-1$. We have $-1\neq 1$, otherwise $2=0$, and a cannot have order 3.

$k=4$: We have $(1+a)^4=1+4a+6a^2+4a^3+a^4=1+4a+6a^2+4+a=5(1+a+a^2)+a^2=a^2$, which is not equal to 1, as a would have been order 2 otherwise.

$k=5$: We have $(1+a)^5=1+5a+10a^2+10a^3+5a^4+a^5=1+5a+10a^2+10+5a+a^2=11+10a+11a^2=11(1+a+a^2)-a=-a$, and $-a\neq 1$, as otherwise $a=-1$, which doesn't have order 3.

$k=6$: We have $(1+a)^6=1+6a+15a^2+20a^3+15a^4+6a^5+a^6=1+6a+15a^2+20+15a+6a^2+1=22+21a+21a^2=1+21(1+a+a^2)=1$.

Ex. 4.23 Show that $x^2\equiv -1 \pmod{p}$ has a solution iff $p\equiv 1 \pmod{4}$, and that $x^4\equiv -1 \pmod{p}$ has a solution iff $p\equiv 1 \pmod{8}$.

For the first congruence, we use Proposition 4.2.1 to conclude that existence of 2nd power residue of -1 modulo prime p is equivalent to $(-1)^{(p-1)/2}\equiv 1 \pmod{p}$, which in turn is equivalent to $(p-1)/2$ being even, that is, $p\equiv 1 \pmod{4}$.

We do the same for the second congruence: -1 is a 4th power residue modulo p if $(-1)^{(p-1)/d}\equiv 1 \pmod{p}$, where $d=(4,p-1)$. Note that if a is 4th power residue, then it is 2nd power reside too, so necessarily $p\equiv 1 \pmod{4}$, and so $d=4$. Therefore, we are asking when $(-1)^{(p-1)/4}\equiv 1 \pmod{p}$, which in turn is equivalent to $(p-1)/4$ being even, which happens whenever $p\equiv 1 \pmod{8}$.

Ex. 4.24 Show that $ax^m+by^n\equiv c \pmod{p}$ has the same number of solutions as $ax^{m'}+by^{n'}\equiv c \pmod{p}$, where $m'=(m,p-1)$ and $n'=(n,p-1)$.

5 Chapter 5

Ex. 5.1 Use Gauss' lemma to determine $\left(\frac{5}{7}\right), \left(\frac{3}{11}\right), \left(\frac{6}{13}\right), \left(\frac{-1}{p}\right)$.

$\left(\frac{5}{7}\right)$: $(7-1)/2=3$, and so least residues of $1\cdot 5, 2\cdot 5, 3\cdot 5$ are $-2, 3, 1$ respectively, so $\mu=1$ and $\left(\frac{5}{7}\right)=(-1)^\mu=-1$.

$\left(\frac{3}{11}\right)$: $(11-1)/2 = 5$, and so least residues of $1\cdot 3, 2\cdot 3, 3\cdot 3, 4\cdot 3, 5\cdot 3$ are $3, -1, -2, 1, 4$ respectively, so $\mu = 2$ and $\left(\frac{3}{11}\right) = (-1)^\mu = 1$.

$\left(\frac{6}{13}\right)$: $(13-1)/2 = 6$, the least residues of first 6 multiples of 6 are $1, -1, 6, -2, 4, -3$, $\mu = 3$, $\left(\frac{6}{13}\right) = (-1)^\mu = -1$.

$\left(\frac{-1}{p}\right)$: the least residues of the first $(p-1)/2$ multiples of -1 are all negative, so $\left(\frac{-1}{p}\right) = (-1)^\mu = (-1)^{(p-1)/2}$.

Ex. 5.2 Show that the number of solutions to $x^2 \equiv a \pmod p$ is equal to $1 + (a/p)$.

If x is a solution to the given congruence, $-x$ is also a solution, and it's a different solution unless $x \equiv 0$ or $x \equiv -x \pmod p$, but p is odd, so it cannot happen. Since the equation is of degree 2 over a field, there cannot be any more solutions.

If $a \equiv 0 \pmod p$, there's only one solution, $x \equiv 0 \pmod p$, but also $1 + (0/p) = 1 + 0 = 1$.

Otherwise, there are either 0 or 2 solutions. There are 0 solutions whenever a is not a quadratic residue, that is, $(a/p) = -1$, and $1 + (a/p) = 1 + (-1) = 0$ in that case. In the other case, $(a/p) = 1$, and so $1 + (a/p) = 1 + 1 = 2$. In all cases the expression $1 + (a/p)$ equals the number of solutions.

Ex. 5.3 Suppose $p \not| a$. Show that the number of solutions to $ax^2 + bx + c \equiv 0 \pmod p$ is equal to $1 + (b^- 4ac/p)$.

High school algebra gives tells us that the solutions correspond to quadratic residues of $\Delta = b^2 - 4ac$, and so we can just use the result from the previous exercise.

Ex. 5.4 Prove that $\sum_{a=1}^{p-1}(a/p) = 0$.

This is clear: there are exactly as many quadratic residues as there are nonresidues, and for residues $(a/p) = 1$, and for nonresidues it equals -1.

Ex. 5.5 Prove that $\sum_{x=1}^{p-1}((ax+b)/p) = 0$ provided that $p \not| a$.

If $p \not| a$, then $\{a\cdot 1, a\cdot 2, \ldots, a\cdot(p-1)\}$ is a complete set of residues modulo p, and thus also is $\{a\cdot 1 + b, a\cdot 2 + b, \ldots, a\cdot(p-1) + b\}$, so we just use the result of the previous exercise.

Ex. 5.6 Show that the number of solutions to $x^2 - y^2 \equiv a \pmod p$ is given by:

$$\sum_{y=0}^{p-1}(1 + ((y^2 + a)/p)) \tag{76}$$

This is pretty clear: the equation is equivalent to $x^2 \equiv y^2 + a \pmod p$, which, if we hold y fixed, by Ex. 5.2 has $(1 + ((y^2 + a)/p))$, so if we let y vary from 1 to $p-1$ and sum the number of solutions for each y, we get the result.

Ex. 5.7 By calculating directly show that the number of solutions to $x^2 - y^2 \equiv a \pmod p$ is $p-1$ if $p \not| a$, and $2p-1$ if $p|a$.

We change variables $u = x + y$, $v = x - y$. The equation then takes form $uv \equiv a \pmod p$.

If $p|a$, that is, $a \equiv 0 \pmod p$, then there are exactly $2p-1$ solutions corresponding to $u = 0$ and any v, to $v = 0$ and any u. Each of these gives us p solutions, but we get $u = v = 0$ for both, so there are $2p-1$ solutions overall. All of these are obtainable from original variables: we obtain $u = 0$ and any v by letting $x = -y = v\cdot 2^{-1}$, and $v = 0$ and any u by letting $x = y = u\cdot 2^{-1}$.

Otherwise, if $p \not| a$, as we fix v and vary u from 1 to $p-1$, the values of uv are all nonzero residues mod p. Exactly one of them is congruent to a. We can fix v to $p-1$ different values, and so we get $p-1$ different solutions. Note also that our variable substitution is bijective.

Ex. 5.8 Combining the results of Ex. 5.6 and 5.7 show that:

$$\sum_{y=0}^{p-1}\left(\frac{y^2 + a}{p}\right) = \begin{cases} -1 & \text{if } p \not| a \\ p-1 & \text{if } p|a \end{cases} \tag{77}$$

Immediate.

Ex. 5.9 Prove that $1^2 3^2 \cdots (p-2)^2 \equiv (-1)^{(p-1)/2} \pmod{p}$ using Wilson's theorem.

Note that $a^2 \equiv a(a-p) \equiv -a(p-a) \pmod{p}$, and so:

$$1^2 3^2 \cdots (p-2)^2 \equiv (-1)^{(p-1)/2} 1(p-1)3(p-3)\cdots(p-2)2 \equiv (-1)^{(p-1)/2}(-1) \equiv (-1)^{(p+1)/2} \pmod{p} \quad (78)$$

Ex. 5.10 Let $r_1, r_2, \ldots, r_{(p-1)/2}$ be the quadratic residues between 1 and p. Show that their product is congruent to 1 modulo if $p \equiv 3 \pmod{4}$, and to -1 if $p \equiv 1 \pmod{4}$.

This is the same problem as Ex 5.9 – $1^2, 3^2, \ldots, (p-2)^2$ are all quadratic residues, as each quadratic residue is a square of two different residues, namely a and $p-a$, at least one of which occurs on the list above.

Ex. 5.11 Suppose that $p \equiv 3 \pmod{4}$, and that $q = 2p+1$ is also prime. Prove that $2^p - 1$ is not prime.

We'll show that $2^p \equiv 1 \pmod{q}$. Note that $p = (q-1)/2$, and so $2^p = 2^{(q-1)/2} \equiv (2/q) \pmod{q}$. Consider then $(2/q)$. It is equal to $(-1)^{(q^2-1)/8}$. The exponent is equal to $(4p^2+4p)/8 = (p^2+p)/2$. Since $p \equiv 3 \pmod{4}$, $p^2+p \equiv 0 \pmod{4}$, and so $(p^2+p)/2$ is even. Therefore $(2/q) = 1$, and so $2^p \equiv (2/q) = 1 \pmod{q}$.

Ex. 5.12 Let $f(x) \in \mathbb{Z}[x]$. We say that a prime p divides $f(x)$ if there's an integer n such that $p|f(n)$. Describe the prime divisors of x^2+1 and x^2-2.

We are asking for which p, $x^2+1 \equiv 0 \pmod{p}$, and for which p, $x^2-2 \equiv 0 \pmod{p}$. This is equivalent to asking for which p, -1 and 2 are quadratic residue. Quadratic reciprocity answers these questions in a satisfactory way.

Ex. 5.13 Show that any prime divisor of $x^4 - x^2 + 1$ is congruent to 1 modulo 12.

Suppose that x is such that $x^4 - x^2 + 1 \equiv 0 \pmod{p}$. We use Ex. 5.3 to conclude that $1^2 - 4 \cdot 1 \cdot 1 = -3$ is a quadratic residue modulo p, that is, $(-3/p) = 1$. We have:

$$1 = \left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{(p-1)/2}\left(\frac{3}{p}\right) \quad (79)$$

On the other hand, the quadratic reciprocity tells us that:

$$\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{(3-1)/2 \cdot (p-1)/2} = (-1)^{(p-1)/2} \quad (80)$$

Combining (79) with (80), we get:

$$\left(\frac{p}{3}\right) = 1 \quad (81)$$

This implies that $p \equiv 1 \pmod{3}$. It remains to prove that $p \equiv 1 \pmod{4}$, which is equivalent to showing that -1 is a quadratic residue modulo p.

Write the original equation in the form $x^2(x^2-1) \equiv -1 \pmod{p}$. As x^2 is obviously a quadratic residue, if we show that $x^2 - 1$ is also a quadratic residue, then -1 will also be a quadratic residue, as a product of two residues.

But again we rewrite the original equation as $x^4 \equiv x^2 - 1 \pmod{p}$, from which it is clear that $x^2 - 1$ is a quadratic (even biquadratic) residue.

Ex. 5.14 Use the fact that $U(\mathbb{Z}/p\mathbb{Z})$ is cyclic to give a direct proof that $(-3/p) = 1$ when $p \equiv 1 \pmod{3}$.

Since $p \equiv 1 \pmod{3}$, 3 divides $p-1$, and so by Cauchy theorem, there's an element $\rho \in U(\mathbb{Z}/p\mathbb{Z})$ of order 3. We'll show that $(2\rho+1)^2 \equiv -3 \pmod{p}$.

Since $\rho^3 \equiv 1$, $1 + \rho + \rho^2 \equiv 0$. Then $4\rho^2 + 4\rho + 4 \equiv 0$, so $(2\rho+1)^2 \equiv -3$.

Ex. 5.15 If $p \equiv 1 \pmod{5}$, show directly that $(5/p) = 1$ by the method of Ex. 5.14.

Since $p \equiv 1 \pmod{5}$, 5 divides $p-1$, and so by Cauchy theorem, there's an element $\rho \in U(\mathbb{Z}/p\mathbb{Z})$ of order 5.

Since ρ has order 5, $1+\rho+\rho^2+\rho^3+\rho^4 = 0$. Then, simple calculation shows that $(\rho+\rho^4)^2+(\rho+\rho^4)-1 = 0$. This means that $x^2 + x - 1 \equiv 0 \pmod{p}$ is solvable, which by Ex. 4.3 is equivalent to $1^2 - 4 \cdot 1 \cdot (-1) = 5$ being a quadratic residue.

Ex. 5.16 Using quadratic reciprocity find the primes for which 7 is quadratic residue. Do the same for 15.

Quadratic reciprocity tells us that:

$$\left(\frac{p}{7}\right)\left(\frac{7}{p}\right) = (-1)^{(p-1)/2\cdot(7-1)/2} = (-1)^{3(p-1)/2} = (-1)^{(p-1)/2} \tag{82}$$

Let us now consider $(p/7)$. The quadratic residues modulo 7 are $1, 2, 4$. Thus, $(7/p) = 1$ whenever p is congruent to either of $1, 2, 4$ modulo 7 and 1 modulo 4, or to $3, 5, 6$ modulo 7 and 3 modulo 4. We can sum up these conditions to: p must be congruent to either of $1, 2, 4, 9, 15, 18$ modulo 28.

The process for 15 is mostly the same, save for a minor details that 15 is actually not a prime. However, we note that $(15/p) = (3/p)(5/p)$, and then we proceed to determine the quadratic character of 3 and 5.

Ex. 5.17 Supply the details to the proof of Proposition 5.2.1 and to the corollary to the lemma following it.

This is too trivial to bother writing it down.

Ex. 5.18 Let D be a square-free integer that is also odd and positive. Show that there's an integer b prime to D such that $(b/D) = -1$.

Let $D = p_1 \cdots p_k$. By definition:

$$\left(\frac{b}{D}\right) = \left(\frac{b}{p_1}\right)\cdots\left(\frac{b}{p_k}\right) \tag{83}$$

Let b_1 be any quadratic non-residue modulo p_1, and b_i for $i > 1$ be any quadratic residues modulo p_i. By Chinese remainder theorem, there exists b such that $b \equiv b_i \pmod{p_i}$, and by (83), it is clear that $(b/D) = -1$.

Ex. 5.19 Let D be as in Exercise 18. Show that $\sum(a/D) = 0$, where the sum is over a reduced residue system modulo D. Conclude that exactly one half of the elements in $U(\mathbb{Z}/D\mathbb{Z})$ satisfy $(a/D) = 1$.

If D is prime itself, then the proposition follows from the corresponding property of the regular Legendre symbol (there are exactly as many residues as there are nonresidues). Therefore, let $D = p_1 \ldots p_k$, p_i be all different, and $k > 1$. Let $D' = p_2 \ldots p_k$, so that $D = p_1 D'$. Then:

$$\sum_{\text{mod } D}\left(\frac{a}{D}\right) = \sum_{\text{mod } D}\left(\frac{a}{p_1}\right)\left(\frac{a}{D'}\right) \tag{84}$$

where $\sum_{\text{mod } D}$ denotes sum over reduced residues modulo D.

By Chinese remainder theorem, each reduced residue a modulo D corresponds to a pair of (residue modulo p_1, residue modulo D') through coordinate-wise reduction. All residues modulo D arise this way. Thus, we can write:

$$\sum_{\text{mod } D}\left(\frac{a}{p_1}\right)\left(\frac{a}{D'}\right) = \left(\sum_{\text{mod } p_1}\left(\frac{a}{p_1}\right)\right)\left(\sum_{\text{mod } D'}\left(\frac{a}{D'}\right)\right) \tag{85}$$

But now again $\sum_{\text{mod } p_1}\left(\frac{a}{p_1}\right) = 0$ by properties of regular Legendre symbol, so the whole sum must be 0.

Since $\sum_{\text{mod } D}\left(\frac{a}{D}\right) = 0$, and each summand is either 1 or -1, there must be exactly as many 1s as there are -1s.

Ex. 5.20 Let $a_1, a_2, \ldots, a_{\phi(D)/2}$ be integers between 1 and D such that $(a_i, D) = 1$ and $(a_i/D) = 1$. Prove that D is a quadratic residue modulo a prime $p \nmid D$, $p \equiv 1 \pmod 4$ iff $p \equiv a_i \pmod{D}$ for some i.

We are interested in calculating (D/p). Generalization of quadratic reciprocity to Jacobi symbol gives us the following relation:

$$\left(\frac{p}{D}\right)\left(\frac{D}{p}\right) = (-1)^{\frac{p-1}{2}\frac{D-1}{2}} = 1 \tag{86}$$

Thus $(D/p) = (p/D)$. But $(p/D) = 1$ exactly if $p \equiv a_i \pmod{D}$ for some i.

Ex. 5.21 Apply the method of Ex. 5.19 and 5.20 to find those primes for which 21 is a quadratic residue.

Let $D = 21 = 3 \cdot 7$, $\phi(21) = (3-1)(7-1) = 2 \cdot 6 = 12$. Thus there are $\phi(21)/2 = 6$ residues a modulo 21 such that $(a/21) = 1$. These are either residues, which are quadratic residues of both 3 and 7, or residues which are quadratic nonresidues of both 3 and 7. There's a single quadratic residue mod 3, which is 1, and a single nonresidue, which is 2. There are 3 quadratic residues mod 7, which are 1, 2, and 4, and 3 nonresidues, which are 3, 5 and 6. Thus, if a is such that $(a/21) = 1$, then these are the possibilities for values of $(a \mod 3, a \mod 7)$: $(1,1), (1,2), (1,4), (2,3), (2,5), (2,6)$. We can recover residues mod 21 from these pairs using Chinese remainder theorem. Then, the solution to exercise amounts to applying the previous exercise.

Ex. 5.22 Use the Jacobi symbol to determine (113/997), (215/761), (514/1093), and (401/757).

We'll do only the first one, (113/997). We have:

$$\left(\frac{113}{997}\right)\left(\frac{997}{113}\right) = (-1)^{\frac{113-1}{2}\frac{997-1}{2}} = (-1)^{56 \cdot 498} = 1 \tag{87}$$

Thus $(113/997) = (997/113) = (93/113)$. We apply reciprocity again:

$$\left(\frac{93}{113}\right)\left(\frac{113}{93}\right) = (-1)^{\frac{93-1}{2}\frac{113-1}{2}} = (-1)^{46 \cdot 56} = 1 \tag{88}$$

Thus $(93/113) = (113/93) = (20/93) = (4/93) \cdot (5/93) = (5/93)$, as 4 is always a quadratic residue. Thus we have:

$$\left(\frac{5}{93}\right)\left(\frac{93}{5}\right) = (-1)^{\frac{93-1}{2}\frac{5-1}{2}} = (-1)^{46 \cdot 2} = 1 \tag{89}$$

And so $(5/93) = (93/5) = (3/5) = -1$, as $1, 4$ are the only quadratic residues modulo 5.

Ex. 5.23 Suppose that $p \equiv 1 \pmod 4$. Show that there exist integers s and t such that $pt = 1 + s^2$. Conclude that p is not a prime in $\mathbb{Z}[i]$. Remember that $\mathbb{Z}[i]$ has unique factorization.

Since $p \equiv 1 \pmod 4$, $(-1)^{(p-1)/2} = 1$, and so -1 is a quadratic residue. Thus there exists $s \leqslant p-1$ such that $s^2 \equiv -1 \pmod p$, which is the same as saying that p divides $s^2 + 1$, that is, $pt = s^2 + 1$.

In $\mathbb{Z}[i]$ we can factor $pt = s^2 + 1$ as $pt = (s-i)(s+i)$. If p was a prime, it would have to divide one of $s+i, s-i$, and so $p^2 = ||p|| \leqslant \max(||s-i||, ||s+i||) = \max(s^2+1, s^2+1) = s^2 + 1 \leqslant p^2 - 2p + 1 + 1$, and so $2p \leqslant 2$, which is a contradiction.

Ex. 5.24 If $p \equiv 1 \pmod 4$, show that p is a sum of two squares, i.e. $p = a^2 + b^2$ with $a, b \in \mathbb{Z}$.

Since p is a nonprime in $\mathbb{Z}[i]$, we can write $p = \alpha\beta$ for some nonunit $\alpha, \beta \in \mathbb{Z}[i]$. We then have:

$$p^2 = ||p|| = ||\alpha\beta|| = ||\alpha|| \cdot ||\beta|| = (x^2 + y^2)(c^2 + d^2) \tag{90}$$

Since p is prime, both sides of above equality are integers, and neither α nor β are units, we must have $p = x^2 + y^2 = c^2 + d^2$. Now it only remains to show that neither of, say, x or y, is 0. If $y = 0$, then $\alpha \in \mathbb{Z}$, and so $\beta \in \mathbb{Z}$, cause otherwise if $\beta \notin \mathbb{Z}$, $p = \alpha\beta \notin \mathbb{Z}$, which is a contradiction. But if $\alpha, \beta \in \mathbb{Z}$, they would give a nontrivial factorization of p in $\mathbb{Z}$, which cannot exist. We deal with the case of $x = 0$ by similar argument.

Ex. 5.25 An integer is called a biquadratic residue modulo p if it is congruent to a fourth power. Using the identity $x^4 + 4 = ((x+1)^2 + 1)((x-1)^2 + 1)$ show that -4 is a biquadratic residue modulo p iff $p \equiv 1 \pmod 4$.

In one direction it's trivial: if -1 is a biquadratic residue, it necessarily is also a quadratic residue, and so $p \equiv 1 \pmod 4$. In the other direction, assume that $p \equiv 1 \pmod 4$, so that -1 is a quadratic residue. Thus there's an x such that $(x+1)^2 \equiv -1 \pmod p$, and so $x^2 + 4 \equiv ((x+1)^2 + 1)((x-1)^2 + 1) \equiv 0 \pmod p$, that is, -4 is a biquadratic residue.

Ex. 5.26 This exercise and Ex. 5.27 and 5.28 give Dirichlet's beautiful proof that 2 is a biquadratic residue modulo p iff p can be written in the form $A^2 + 64B^2$, where $A, B \in \mathbb{Z}$. Suppose that $p \equiv 1 \pmod 4$. Then $p = a^2 + b^2$ by Ex. 5.24. Take a to be odd. Prove the following statements:

a) $(a/p) = 1$.

b) $((a+b)/p) = (-1)^{((a+b)^2-1)/8}$.

c) $(a+b)^2 \equiv 2ab \pmod{p}$

d) $(a+b)^{(p-1)/2} \equiv (2ab)^{(p-1)/4} \pmod{p}$.

We'll begin with proving $(a/p) = 1$. Since a is odd, we can use quadratic reciprocity theorem with Jacobi symbols:

$$\left(\frac{a}{p}\right)\left(\frac{p}{a}\right) = (-1)^{\frac{p-1}{2}\frac{a-1}{2}} = 1 \tag{91}$$

Thus $(a/p) = (p/a)$. On the other hand, as $p - b^2 = a^2$, $p \equiv b^2 \pmod{a}$, and so $(p/a) = (b^2/a) = 1$, which proves a).

We now focus on b). We proceed similarly as in a): using quadratic reciprocity, since $a+b$ is odd, we have $((a+b)/p) = (p/(a+b))$. On the other hand, since $2p = (a+b)^2 + (a-b)^2$, we have $2p \equiv (a-b)^2 \pmod{a+b}$, and so $(2p/(a+b)) = ((a-b)^2/(a+b)) = 1$. But since $(2p/(a+b)) = (2/(a+b))(p/(a+b))$, $(p/(a+b)) = (2/(a+b))$, and $(2/(a+b)) = (-1)^{\frac{(a+b)^2-1}{8}}$.

We proceed to c), which is pretty trivial: $(a+b)^2 = a^2+b^2+2ab = p+2ab$, from which the congruence in c) follows immediately. The congruence from d) also follows immediately from c).

Ex. 5.27 Suppose that f is such that $b \equiv af \pmod{p}$. Show that $f^2 \equiv -1 \pmod{p}$, and that $2^{(p-1)/4} \equiv f^{ab/2} \pmod{p}$.

If $b \equiv af \pmod{p}$. then $0 = (b-af)(b+af) = b^2 - f^2a^2 \pmod{p}$, so $b^2 \equiv f^2a^2 \pmod{p}$. But from $p = a^2+b^2$ we know that $b^2 \equiv -a^2 \pmod{p}$, and so $-a^2 \equiv f^2a^2 \pmod{p}$, and since $a \not\equiv 0 \pmod{p}$, $-1 \equiv f^2 \pmod{p}$.

Combining b) with d) from the previous exercise, we get that:

$$(-1)^{(p-1+2ab)/8} = (-1)^{((a+b)^2-1)/8} = ((a+b)/p) \equiv (a+b)^{(p-1)/2} \equiv (2ab)^{(p-1)/4} \pmod{p}. \tag{92}$$

For the left hand side, we have:

$$(-1)^{(p-1+2ab)/8} \equiv (f^2)^{(p-1+2ab)/8} = f^{(p-1+2ab)/4} \pmod{p} \tag{93}$$

On the other hand, as $b \equiv af \pmod{p}$,

$$(2ab)^{(p-1)/4} \equiv (2a^2f)^{(p-1)/4} = (2f)^{(p-1)/4}a^{(p-1)/2} \equiv (2f)^{(p-1)/4} \pmod{p}, \tag{94}$$

since a is a quadratic residue mod p.

We thus get:

$$f^{(p-1+2ab)/4} \equiv (2f)^{(p-1)/4} \pmod{p} \tag{95}$$

and so dividing both sides by $f^{(p-1)/4}$, we get:

$$f^{ab/2} \equiv 2^{(p-1)/4} \pmod{p}, \tag{96}$$

which is a desired conclusion.

Ex. 5.28 Show that $x^4 \equiv 2 \pmod{p}$ has a solution for $p \equiv 1 \pmod{4}$ iff p is of the form $A^2 + 64B^2$.

We note that 2 is a biquadratic residue precisely when $2^{(p-1)/4} \equiv 1 \pmod{p}$. By previous exercise, $2^{(p-1)/4} \equiv f^{ab/2} \pmod{p}$, a, b and f are such that $p = a^2+b^2$, a is odd, and $b \equiv af \pmod{p}$. Now since $f^2 \equiv -1 \pmod{p}$ by previous exercise, $f^{ab/4} \equiv 1 \pmod{p}$ precisely when $ab/2$ is divisible by 4, but since a is odd, it happens precisely when b is divisible by 8. Thus we get a conclusion: 2 is a biquadratic residue precisely when $b = 8B$, that is, when $p = A^2 + 64B^2$ for $A = a$ and $B = b/8$.

Ex. 5.29 Let (RR) be the number of pairs $(n, n+1)$ in the set $1, 2, 3, \ldots, p-1$ such that n and $n+1$ are both quadratic residues modulo p. Let (NR) be the number of pairs $(n, n+1)$ in the set $1, 2, 3, \ldots, p-1$ such that n is a quadratic nonresidue and $n+1$ is a quadratic residue. Similarly, define (RN) and (NN). Determine the sums $(RR)+(RN)$, $(NR)+(NN)$, $(RR)+(NR)$, and $(RN)+(NN)$.

This is actually pretty obvious: consider $(RR)+(RN)$. For every quadratic residue $n < p-1$, either $n+1$ is a quadratic residue, in which case it contributes 1 to (RR), or it isn't, in which case it contributes 1 to (RN). Thus $(RR)+(RN)$ is the number of quadratic residues smaller than $p-1$, which is $(p-1)/2 = (p-2-(-1))/2$ when -1 is a quadratic nonresidue, and $(p-1)/2 - 1 = (p-2-1)/2$

when -1 is a quadratic residue. Since -1 is a quadratic residue precisely when $\epsilon = (-1)^{(p-1)/2} = 1$, we can represent these to cases using a single formula $(RR) + (RN) = (p - 2 - \epsilon)/2$.

The argunent in case $(NR) + (NN)$ is pretty much the same: every nonresidue smaller than $p - 1$ contributes 1 to the sum, so $(NR) + (NN)$ is the number of nonresidues smaller than $p - 1$, and so the result is $(NR) + (NN) = (p - 2 + \epsilon)/2$.

For $(RR) + (NR)$ there's a little twist: if $n + 1 > 1$ is a quadratic residue, then if n is a residue too, then it contributes one to (RR), and if it's not, it contributes one to (NR). Thus, every residue $n \geqslant 2$ contributes 1 to $(RR) + (NR)$. Since 1 is always a quadratic residue, there are exactly $(p - 1)/2 - 1$ residues larger than 1, so $(RR) + (NR) = (p - 3)/2$.

On the other hand, the sum $(RN)+(NN)$ is always exactly $(p-1)/2$: when considering pairs $(n, n+1)$, all nonresidues can always occur as $n + 1$.

Similar argument tells us that $(RR) + (RN) + (NR) + (NN)$ is exactly $p - 2$: there are $p - 2$ pairs of the form $(n, n + 1)$ with $n, n + 1$ in $1, 2, \ldots, p - 1$, and each $(n, n + 1)$ contributes to exactly one of $(RR), (RN), (NR), (NN)$. On the other hand, if we add all the sums we calculated beforehand, we get:

$$\begin{aligned}
2(p-2) &= 2((RR) + (RN) + (NR) + (NN)) && (97)\\
&= ((RR) + (RN)) + ((NR) + (NN)) + ((RR) + (NR)) + ((RN) + (NN)) && (98)\\
&= \frac{p - 2 - \epsilon + p - 2 + \epsilon + p - 3 + p - 1}{2} && (99)\\
&= \frac{4p - 8}{2} = 2p - 4 && (100)
\end{aligned}$$

And so it seems that we got it basically correct.

Ex. 5.30 Show that $(RR) + (NN) - (RN) - (NR) = \sum_{n=1}^{p-1}(n(n + 1)/p)$. Evaluate this sum and show that it is equal to -1.

Note there's a misprint in the book that says that the sum is $\sum_{n=1}^{p-1}(n(n + 1))/p$, so that we're not summing Legendre symbols. In that case, once we evaluate the sum, we get the following:

$$\begin{aligned}
\sum_{n=1}^{p-1} \frac{n(n+1)}{p} &= \sum_{n=1}^{p-1} \frac{n^2 + n}{p} && (101)\\
&= \frac{1}{p}\left(\frac{p(p+1)(2p+1)}{6} + \frac{p(p+1)}{2}\right) && (102)\\
&= \frac{(p+1)(2p+1) + 3(p+1)}{6} && (103)\\
&= \frac{(p+1)(2p+5)}{6} && (104)
\end{aligned}$$

I don't even see how this is an integer.

So, we'll show that the given sum is actually equal to $\sum_{n=1}^{p-1}(n(n + 1)/p)$, but this is pretty immediate: $(n(n + 1)/p) = (n/p)((n + 1)/p)$, and this product equals 1 if either both or none of $n, n + 1$ are quadratic residue, and it equals -1 if exactly one of them is a quadratic residue. Thus, each summand in $\sum_{n=1}^{p-2}(n(n + 1)/p)$ represent a single pair $(n, n + 1)$, and contributes exactly 1 to exactly one of $(RR), (NN), -(NR), -(RN)$. We can easily extend the summation to $p - 1$, as $((p - 1)p/p) = 0$.