Solutions to Ireland, Rosen “A Classical Introduction to Modern Number Theory”

Adam Michalik

25 grudnia 2016

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 $f_1, \dots, f_n$ 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 $f_1, \dots, f_n$ 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 $p_1, \dots, p_t$ 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 $ord_p n! = [n/p] + [n/p^2] + [n/p^3] + \dots$.

Since $n!$ is a product of $1, 2, 3, \dots, n$, 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 $p_1, \dots, p_n$ 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 $p, 2p, 3p, \dots, p^{n-1}p^n$. 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:

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

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.