

Contents

0	Prerequisites	0–1
0.1	The number sets	0–1
0.2	The natural numbers	0–1
0.3	Divisibility	0–2
1	The Fundamental Theorem of Arithmetic	1–1
1.1	Primes	1–1
1.2	The fundamental theorem	1–1
1.3	Euclid’s Algorithm	1–2
1.4	Speeding up the algorithm	1–4
1.5	Example	1–5
1.6	An alternative proof	1–6
1.7	Euclid’s Lemma	1–7
1.8	Proof of the Fundamental Theorem	1–7
1.9	A postscript	1–8
2	Euclid’s Theorem	2–1
2.1	Variants on Euclid’s proof	2–1
2.2	Euler’s Product Formula	2–2
3	The Prime Number Theorem	3–1
3.1	The Theorem	3–1
3.2	A little history	3–2
3.3	Alternative version	3–4
3.4	Dirichlet’s Theorem	3–6
4	Fermat and Mersenne Primes	4–1
4.1	Fermat primes	4–1
4.2	Mersenne primes	4–2
4.3	Perfect numbers	4–4

5	Modular arithmetic	5–1
5.1	The modular ring	5–1
5.2	The prime fields	5–2
5.3	The additive group	5–3
5.4	The multiplicative group	5–4
5.5	Homomorphisms	5–7
5.6	Finite fields	5–7
6	The Chinese Remainder Theorem	6–1
6.1	Coprime moduli	6–1
6.2	The modular ring	6–3
6.3	The totient function	6–3
6.4	The multiplicative group	6–5
6.5	Multiple moduli	6–5
7	Polynomial Rings	7–1
7.1	Polynomials	7–1
7.2	Long division	7–1
7.3	Irreducibility	7–2
7.4	The Euclidean Algorithm for polynomials	7–2
7.5	Unique factorisation	7–3
7.6	Gauss' Lemma	7–4
8	Fermat's Little Theorem	8–1
8.1	Lagrange's Theorem	8–1
8.2	Euler's Theorem	8–2
8.3	Fermat's Little Theorem	8–2
8.4	Carmichael numbers	8–2
8.5	The Miller-Rabin test	8–4
9	Primitive Roots	9–1
9.1	The multiplicative group of a finite field	9–1
9.2	Primitive roots	9–3
9.3	Prime power moduli	9–5
9.4	Carmichael numbers, again	9–8
10	Quadratic Residues	10–1
10.1	Introduction	10–1
10.2	Prime moduli	10–1
10.3	The Legendre symbol	10–3
10.4	Euler's criterion	10–3

10.5	Computing $\left(\frac{a}{p}\right)$	10-5
10.6	$a = -1$	10-6
10.7	$a = 2$	10-7
10.8	Hensel's Lemma	10-9
11	Quadratic Reciprocity	11-1
11.1	Gauss' Law of Quadratic Reciprocity	11-1
11.2	Wilson's Theorem	11-1
11.3	Rousseau's proof	11-2
12	Gaussian Integers	12-1
12.1	Gaussian Numbers	12-1
12.2	Conjugates and norms	12-1
12.3	Units	12-3
12.4	Division in Γ	12-4
12.5	The Euclidean Algorithm in Γ	12-5
12.6	Unique factorisation	12-6
12.7	Re-defining 'prime'	12-7
12.8	Gaussian primes	12-8
12.9	Sums of squares	12-11
13	Algebraic numbers and algebraic integers	13-1
13.1	Algebraic numbers	13-1
13.2	Algebraic integers	13-2
13.3	Number fields and number rings	13-4
14	Quadratic fields and quadratic number rings	14-1
14.1	Quadratic number fields	14-1
14.2	Conjugacy	14-3
14.3	Quadratic number rings	14-4
14.4	Units I: Imaginary quadratic fields	14-6
15	Pell's Equation	15-1
15.1	Kronecker's Theorem	15-1
15.2	Pell's Equation	15-2
15.3	Units II: Real quadratic fields	15-5
16	$Q(\sqrt{5})$ and the golden ratio	16-1
16.1	The field $Q(\sqrt{5})$	16-1
16.2	The number ring $Z[\phi]$	16-2
16.3	Unique Factorisation	16-2

16.4	The units in $\mathbb{Z}[\phi]$	16–4
16.5	The primes in $\mathbb{Z}[\phi]$	16–5
16.6	Fibonacci numbers	16–7
16.7	The weak Lucas-Lehmer test for Mersenne primality	16–8
17	$\mathbb{Z}[\sqrt{3}]$ and the Lucas-Lehmer test	17–1
17.1	The field $\mathbb{Q}(\sqrt{3})$	17–1
17.2	The ring $\mathbb{Z}[\sqrt{3}]$	17–1
17.3	The units in $\mathbb{Z}[\sqrt{3}]$	17–1
17.4	Unique Factorisation	17–3
17.5	The primes in $\mathbb{Z}[\sqrt{3}]$	17–3
17.6	The Lucas-Lehmer test for Mersenne primality	17–5
18	Continued fractions	18–1
18.1	Finite continued fractions	18–1
18.2	The p 's and q 's	18–2
18.3	Successive approximants	18–4
18.4	Uniqueness	18–7
18.5	A fundamental identity	18–8
18.6	Infinite continued fractions	18–9
18.7	Diophantine approximation	18–11
18.8	Quadratic surds and periodic continued fractions	18–14
A	The Structure of Finite Abelian Groups	1–1
A.1	The Structure Theorem	1–1
A.2	Primary decomposition	1–1
A.3	Decomposition of the primary components	1–3
A.4	Uniqueness	1–5
A.5	Note	1–5

Chapter 6

The Chinese Remainder Theorem

6.1 Coprime moduli

Theorem 6.1. *Suppose $m, n \in \mathbb{N}$, and*

$$\gcd(m, n) = 1.$$

Given any remainders $r \bmod m$ and $s \bmod n$ we can find N such that

$$N \equiv r \bmod m \text{ and } N \equiv s \bmod n.$$

Moreover, this solution is unique mod mn .

Proof. We use the pigeon-hole principle. Consider the mn numbers

$$0 \leq N < mn.$$

For each N consider the remainders

$$r = N \bmod m, \quad s = N \bmod n,$$

where r, s are chosen so that

$$0 \leq r < m, \quad 0 \leq s < n.$$

We claim that these pairs r, s are different for different $N \in [0, mn)$. For suppose $N < N'$ have the same remainders, ie

$$N' \equiv N \bmod m \text{ and } N' \equiv N \bmod n.$$

6.1. COPRIME CHAPTER 6. THE CHINESE REMAINDER THEOREM

Then

$$m \mid N' - N \text{ and } n \mid N' - N.$$

Since $\gcd(m, n) = 1$, it follows that

$$mn \mid N' - N.$$

But that is impossible, since

$$0 < N' - N < mn.$$

□

Example: Let us find N such that

$$N \equiv 3 \pmod{13}, N \equiv 7 \pmod{23}.$$

One way to find N is to find a, b such that

$$\begin{aligned} a &\equiv 1 \pmod{m}, a \equiv 0 \pmod{n}, \\ b &\equiv 0 \pmod{m}, b \equiv 1 \pmod{n}. \end{aligned}$$

For then we can take

$$N = 3a + 7b.$$

Note that

$$a = 1 + sm = tn.$$

We are back to the Euclidean Algorithm for $\gcd(m, n)$:

$$\begin{aligned} 23 &= 2 \cdot 13 - 3, \\ 13 &= 4 \cdot 3 + 1, \end{aligned}$$

giving

$$\begin{aligned} 1 &= 13 - 4 \cdot 3 \\ &= 13 - 4(2 \cdot 13 - 23) \\ &= 4 \cdot 23 - 7 \cdot 13. \end{aligned}$$

Thus we can take

$$a = 4 \cdot 23 = 92, b = -7 \cdot 13 = -91.$$

giving

$$N = 3 \cdot 92 - 7 \cdot 91 = 276 - 637 = -361.$$

Of course we can add a multiple of mn to N ; so we could take

$$N = 13 \cdot 23 - 361 = 299 - 361 = -62,$$

if we want the smallest solution (by absolute value); or

$$N = 299 - 62 = 237,$$

for the smallest positive solution.

6.2 The modular ring

We can express the Chinese Remainder Theorem in more abstract language.

Theorem 6.2. *If $\gcd(m, n) = 1$ then the ring $\mathbb{Z}/(mn)$ is isomorphic to the product of the rings $\mathbb{Z}/(m)$ and $\mathbb{Z}/(n)$:*

$$\mathbb{Z}/(mn) = \mathbb{Z}/(m) \times \mathbb{Z}/(n).$$

Proof. We have seen that the maps

$$N \mapsto N \bmod m \text{ and } N \mapsto N \bmod n$$

define ring-homomorphisms

$$\mathbb{Z}/(mn) \rightarrow \mathbb{Z}/(m) \text{ and } \mathbb{Z}/(mn) \rightarrow \mathbb{Z}/(n).$$

These combine to give a ring-homomorphism

$$\mathbb{Z}/(mn) \rightarrow \mathbb{Z}/(m) \times \mathbb{Z}/(n),$$

under which

$$r \bmod mn \mapsto (r \bmod m, r \bmod n).$$

But we have seen that this map is bijective; hence it is a ring-isomorphism. \square

6.3 The totient function

Proposition 6.1. *Suppose $\gcd(m, n) = 1$. Then*

$$\gcd(N, mn) = \gcd(N, m) \cdot \gcd(N, n).$$

Proof. Let

$$d = \gcd(N, mn).$$

Suppose

$$p^e \parallel d.$$

Then

$$p^e \parallel m \text{ or } p^e \parallel n.$$

Thus the prime-power divisors of d are divided between m and n \square

Corollary 6.1. *If $\gcd(m, n) = 1$ and $N \in \mathbb{Z}$ then*

$$\gcd(N, mn) = 1 \iff \gcd(N, m) = 1 \text{ and } \gcd(N, n) = 1.$$

6.3. THE TOTIENT FUNCTION AND THE CHINESE REMAINDER THEOREM

From this we derive

Theorem 6.3. *Euler's totient function is multiplicative, ie*

$$\gcd(m, n) = 1 \implies \phi(mn) = \phi(m)\phi(n).$$

This gives a simple way of computing $\phi(n)$.

Proposition 6.2. *If*

$$n = \prod_{1 \leq i \leq r} p_i^{e_i},$$

where the primes p_1, \dots, p_r are different and each $e_i \geq 1$. Then

$$\phi(n) = \prod_{i=1}^r p_i^{e_i-1} (p_i - 1).$$

Proof. Since $\phi(n)$ is multiplicative,

$$\phi(n) = \prod_i \phi(p_i^{e_i}).$$

The result now follows from

Lemma 6.1. $\phi(p^e) = p^{e-1}(p - 1)$.

Proof. The numbers $r \in [0, p^e]$ is not coprime to p^e if and only if it is divisible by p , ie

$$r \in \{0, p, 2p, \dots, p^e - p\}.$$

There are

$$[p^e/p] = p^{e-1}$$

such numbers. Hence

$$\phi(p^e) = p^e - p^{e-1} = p^{e-1}(p - 1).$$

□

□

Example: Suppose $n = 1000$.

$$\begin{aligned} \phi(1000) &= \phi(2^3 5^3) \\ &= \phi(2^3) \phi(5^3) \\ &= 2^2(2 - 1) 5^2(5 - 1) \\ &= 4 \cdot 1 \cdot 25 \cdot 4 \\ &= 400; \end{aligned}$$

there are just 400 numbers coprime to 1000 between 0 and 1000.

6.4 The multiplicative group

Theorem 6.4. *If $\gcd(m, n) = 1$ then*

$$(\mathbb{Z}/mn)^\times = (\mathbb{Z}/m)^\times \times (\mathbb{Z}/n)^\times.$$

Proof. We have seen that the map

$$r \bmod mn \mapsto (r \bmod m, r \bmod n) : \mathbb{Z}/(mn) \rightarrow \mathbb{Z}/(m) \times \mathbb{Z}/(n)$$

maps r coprime to mn to pairs (r, s) coprime to m, n respectively. Thus the subset $(\mathbb{Z}/mn)^\times$ maps to the product of the subsets $(\mathbb{Z}/m)^\times$ and $(\mathbb{Z}/n)^\times$, from which the result follows. \square

In effect, this is an algebraic expression of the fact that the totient function is multiplicative.

6.5 Multiple moduli

The Chinese Remainder Theorem extends to more than two moduli.

Proposition 6.3. *Suppose n_1, n_2, \dots, n_r are pairwise coprime, ie*

$$i \neq j \implies \gcd(n_i, n_j) = 1;$$

and suppose we are given remainders a_1, a_2, \dots, a_r moduli n_1, n_2, \dots, n_r , respectively. Then there exists a unique $N \bmod n_1 n_2 \cdots n_r$ such that

$$N \equiv a_1 \bmod n_1, N \equiv a_2 \bmod n_2, \dots, N \equiv a_r \bmod n_r.$$

Proof. This follows from the same pigeon-hole argument that we used to establish the Chinese Remainder Theorem.

Or we can prove it by induction on r ; for since

$$\gcd(n_1 n_2 \cdots n_i, n_{i+1}) = 1,$$

we can add one modulus at a time,

Thus if we have found N_i such that

$$N_i \equiv a_1 \bmod n_1, N_i \equiv a_2 \bmod n_2, \dots, N_i \equiv a_i \bmod n_i$$

then by the Chinese Remainder Theorem we can find N_{i+1} such that

$$N_{i+1} \equiv N_i \bmod n_1 n_2 \cdots n_i \text{ and } N_{i+1} \equiv a_{i+1} \bmod n_{i+1}$$

and so

$$N_{i+1} \equiv a_1 \bmod n_1, N_{i+1} \equiv a_2 \bmod n_2, \dots, N_{i+1} \equiv a_{i+1} \bmod n_{i+1},$$

establishing the induction. \square

Example: Suppose we want to solve the simultaneous congruences

$$n \equiv 4 \pmod{5}, \quad n \equiv 2 \pmod{7}, \quad n \equiv 1 \pmod{8}.$$

There are two slightly different approaches to the task.

Firstly, we can start by solving the first 2 congruences. As is easily seen, the solution is

$$n \equiv 9 \pmod{35}.$$

The problem is reduced to two simultaneous congruences:

$$n \equiv 9 \pmod{35}, \quad n \equiv 1 \pmod{8},$$

which we can solve with the help of the Euclidean Algorithm, as before.

Alternatively, we can find solutions of the three sets of simultaneous congruences

$$\begin{aligned} n_1 &\equiv 1 \pmod{5}, \quad n_1 \equiv 0 \pmod{7}, \quad n_1 \equiv 0 \pmod{8}, \\ n_2 &\equiv 0 \pmod{5}, \quad n_2 \equiv 1 \pmod{7}, \quad n_2 \equiv 0 \pmod{8}, \\ n_3 &\equiv 0 \pmod{5}, \quad n_3 \equiv 0 \pmod{7}, \quad n_3 \equiv 1 \pmod{8}, \end{aligned}$$

ie

$$\begin{aligned} n_1 &\equiv 1 \pmod{5}, \quad n_1 \equiv 0 \pmod{56}, \\ n_2 &\equiv 1 \pmod{7}, \quad n_2 \equiv 0 \pmod{40}, \\ n_3 &\equiv 1 \pmod{8}, \quad n_3 \equiv 0 \pmod{35}, \end{aligned}$$

which we can solve by our previous method. The required solution is then

$$n = 4n_1 + 2n_2 + n_3,$$

where the coefficients 4,2,1 are the required residues.

Exercise 6

In exercises 1–10 find the smallest simultaneous solution $n \geq 0$ of the given congruences, or else show that there is no such solution.

- ** 1. $n \equiv 1 \pmod{4}$, $n \equiv 2 \pmod{7}$
- ** 2. $n \equiv 2 \pmod{5}$, $n \equiv 5 \pmod{8}$
- ** 3. $n \equiv 2 \pmod{3}$, $n \equiv 3 \pmod{4}$
- ** 4. $n \equiv 2 \pmod{5}$, $n \equiv 3 \pmod{7}$, $n \equiv 1 \pmod{8}$
- ** 5. $n \equiv 3 \pmod{4}$, $n \equiv 5 \pmod{7}$, $n \equiv 2 \pmod{9}$
- ** 6. $n \equiv 1 \pmod{5}$, $n \equiv 3 \pmod{6}$, $n \equiv 2 \pmod{7}$
- ** 7. $n \equiv 2 \pmod{4}$, $n \equiv 4 \pmod{5}$, $n \equiv 3 \pmod{7}$
- ** 8. $n \equiv 2 \pmod{4}$, $n \equiv 3 \pmod{6}$, $n \equiv 4 \pmod{7}$
- ** 9. $n \equiv 4 \pmod{7}$, $n \equiv 6 \pmod{11}$, $n \equiv 9 \pmod{11}$
- ** 10. $n \equiv 1 \pmod{9}$, $n \equiv 2 \pmod{10}$, $n \equiv 3 \pmod{11}$
- *** 11. How many positive integers $x \leq 10,000$ are there such that the difference $2^x - x^2$ is not divisible by 7?
- *** 12. Show that

$$\phi(n) \rightarrow \infty$$

as $n \rightarrow \infty$.

- **** 13. Find an odd integer k such that $k \cdot 2^n - 1$ is composite for all $n \geq 1$.
- **** 14. Is there a 9-digit number

$$N = d_1d_2 \cdots d_9$$

with the following properties: the 9 digits are distinct, and for each $k \in [1, 9]$ the number

$$d_1d_2 \cdots d_k$$

is divisible by k ?