Chapter 2

Congruences

2.1. Basic congruences

Exercise 2.1.1. Prove that for any real number t there is a unique integer in the interval $[t, t+1)$.

Exercise 2.1.2. Prove that m divides $(n-1)(n-2)\cdots(n-m)$ for every integer n and every integer $m \geq 1$.

Exercise 2.1.3. Suppose that $a_1, \ldots, a_m$ is a complete set of residues mod m. Prove that m divides $(n-a_1)\cdots(n-a_m)$ for every integer n.

Exercise 2.1.4. (a) Explain how "a number of the form $3n-1$" means the same thing as "a number of the form $3n+2$", using the language of congruences.

(b) Prove that the set of integers in the congruence class $a \pmod d$ can be partitioned into the set of integers in the congruence classes $a \pmod{kd}$, $a+d \pmod{kd}, \ldots$ and $a+(k-1)d \pmod{kd}$.

Exercise 2.1.5. Show that if $a \equiv b \pmod m$, then $(a, m) = (b, m)$.

Exercise 2.1.6. Prove that if $a \equiv b \pmod m$, then $a \equiv b \pmod d$ for any divisor d of m.

Exercise 2.1.7. Satisfy yourself that addition and multiplication mod m are commutative.

Exercise 2.1.8. Prove that the property of congruence modulo m is an *equivalence relation* on the integers. To prove this, one must establish

(i) $a \equiv a \pmod m$;
(ii) $a \equiv b \pmod m$ implies $b \equiv a \pmod m$;
(iii) $a \equiv b \pmod m$ and $b \equiv c \pmod m$ imply $a \equiv c \pmod m$.

The equivalence classes are therefore the congruence classes mod m.

Exercise 2.1.9. Under the hypothesis of Lemma 2.1.1, show that $ka+lc \equiv kb+ld \pmod m$ for any integers k and l.

Exercise 2.1.10. If $p|m$ and $m/p \equiv a \pmod q$, then prove that $m \equiv ap \pmod q$.

2.2. The trouble with division

Exercise 2.2.1. Determine one congruence class which gives all solutions to 3 divided by 3 (mod 6). (In other words, find a congruence class $a \pmod m$ such that $3x \equiv 3 \pmod 6$ if and only if $x \equiv a \pmod m$.)

2.3. Congruences for polynomials

Exercise 2.3.1. Prove that $a^k \equiv b^k \pmod m$ for all integers $k \geq 1$, by induction.

Exercise 2.3.2. Deduce, from Corollary 2.3.1, that if $f(t) \in \mathbb{Z}[t]$ and $r, s \in \mathbb{Z}$, then $r - s$ divides $f(r) - f(s)$.

Exercise 2.3.3. Let $f(x) \in \mathbb{Z}[x]$. Suppose that $f(r) \not\equiv 0 \pmod m$ for all integers r in the range $0 \leq r \leq m - 1$. Deduce that there does not exist an integer n for which $f(n) = 0$.

2.4. *Tests for divisibility*

Exercise 2.4.1. (a) Invent tests for divisibility by 2 and 5 (easy).
(b) Invent tests for divisibility by 7 and 13 (similar to the above).
(c)† Create one test that tests for divisibility by 7, 11, and 13 simultaneously (assuming that one knows about the divisibility by 7, 11, and 13 of every non-negative integer up to 1000).

Additional exercises

Exercise 2.5.1. Prove that if a, b, and c are integers and $d = b^2 - 4ac$, then $d \equiv 0$ or $1 \pmod 4$.

Exercise 2.5.2. Prove that if $N = a^2 - b^2$, then either N is odd or N is divisible by 4.

Exercise 2.5.3. (a) Prove that 2 divides $n(3n + 101)$ for every integer n.
(b) Prove that 3 divides $n(2n + 1)(n + 10)$ for every integer n.
(c) Prove that 5 divides $n(n + 1)(2n + 1)(3n + 1)(4n + 1)$ for every integer n.

Exercise 2.5.4. (a) Prove that, for any given integer $k \geq 1$, exactly k of any km consecutive integers is $\equiv a \pmod m$.
(b)† Let I be an interval of length N. Prove that the number of integers in I that are $\equiv a \pmod m$ is between $N/m - 1$ and $N/m + 1$.
(c) By considering the number of even integers in $(0, 2)$ and then in $[0, 2]$, show that (b) cannot be improved, in general.

Exercise 2.5.5. The *Universal Product Code* (that is, the bar code used to identify items in the supermarket) has 12 digits, each between 0 and 9, which we denote by $d_1, \dots, d_{12}$. The first 11 digits identify the product. The 12th is chosen to be the least residue of

$$3d_1 - d_2 + 3d_3 - d_4 - \cdots - d_{10} + 3d_{11} \pmod{10}.$$

(a) Deduce that $d_1 + 3d_2 + d_3 + \cdots + d_{11} + 3d_{12}$ is divisible by 10.
(b) Deduce that if the scanner does not read all the digits correctly, then either the sum in (a) will not be divisible by 10 or the scanner has misread at least two digits.

Exercise 2.5.6. (a) Take $f(x) = x^2$ in Corollary 2.3.1 to determine the squares modulo m, for $m = 3, 4, 5, 6, 7, 8, 9,$ and 10. ("The squares modulo m" are those congruence classes (mod m) that are equivalent to the square of at least one congruence class (mod m).)
(b) Show that there are no solutions in integers x, y, z to $x^2 + y^2 = z^2$ with x and y odd.
(c) Show that if $x^2 + y^2 = z^2$, then 3 divides xy.
(d) Show that there are no solutions in integers x, y, z to $x^2 + y^2 = 3z^2$ with $(x, y) = 1$.
(e) Show that there are no solutions in integers x, y, z to $x^2 + y^2 = 666z^2$ with $(x, y) = 1$.
(f) Prove that no integer $\equiv 7 \pmod 8$ can be written as the sum of three squares of integers.

Exercise 2.5.7.† Show that if $x^3 + y^3 = z^3$, then 7 divides xyz.

Binomial coefficients modulo p

Exercise 2.5.8. Use the formula for $\binom{p}{j}$ given in (0.3.1) to prove that p divides $\binom{p}{j}$ for all integers j in the range $1 \le j \le p-1$. This implies that $\frac{1}{p}\binom{p}{j}$ is an integer.

Exercise 2.5.9. (a) Prove that $\binom{p-1}{j} \equiv (-1)^j \pmod p$ for all $j,\ 0 \le j \le p-1$.
(b) Prove that $\frac{1}{p}\binom{p}{j} \equiv (-1)^{j-1}/j \pmod p$ for all $j,\ 1 \le j \le p-1$.

Exercise 2.5.10.† (a) Prove that $\binom{ap}{bp} \equiv \binom{a}{b} \pmod p$ whenever $a, b \ge 0$.
(b) Prove that $\binom{ap+c}{bp+d} \equiv \binom{a}{b}\cdot\binom{c}{d} \pmod p$ whenever $0 \le c, d \le p-1$. (Remember that $\binom{c}{d} = 0$ if $c < d$.)
(c) If $m = m_0 + m_1 p + m_2 p^2 + \cdots + m_k p^k$ and $n = n_0 + n_1 p + \cdots + n_k p^k$ are non-negative integers written in base p, deduce *Lucas's Theorem* (by induction on $k \ge 0$), that

$$\binom{n}{m} \equiv \binom{n_0}{m_0}\binom{n_1}{m_1}\binom{n_2}{m_2}\cdots\binom{n_k}{m_k} \pmod p.$$

Exercise 2.5.11. Deduce from exercise 2.5.8 that $(x+y)^p \equiv x^p + y^p \pmod p$ for all primes p.

Exercise 2.5.12. Prove that $(x+y)^{p-1} \equiv x^{p-1} - yx^{p-2} + \cdots - xy^{p-2} + y^{p-1} \pmod p$.

Exercise 2.5.13. Prove that $(x+y)^{p^k} \equiv x^{p^k} + y^{p^k} \pmod p$ for all primes p and integers $k \ge 1$.

Exercise 2.5.14. (a) Writing a positive integer $n = n_0 + n_1 p + n_2 p^2 + \cdots$ in base p, use exercise 2.5.13 to prove that

$$(x+y)^n \equiv (x+y)^{n_0}(x^p+y^p)^{n_1}(x^{p^2}+y^{p^2})^{n_2}\cdots \pmod p.$$

(b)† Reprove Lucas's Theorem (as in exercise 2.5.10(c)) by studying the coefficient of $x^m y^{n-m}$ in (a).

Exercise 2.5.15. (a) Prove that $(x+y+z)^p \equiv x^p + y^p + z^p \pmod p$.
(b) Deduce that $(x_1 + x_2 + \cdots + x_n)^p \equiv x_1^p + x_2^p + \cdots + x_n^p \pmod p$ for all $n \ge 2$.

The Fibonacci numbers modulo d

Exercise 2.5.16. (a) Prove that the pigeonhole principle is true.
We will now show that the Mersenne numbers $M_n := 2^n - 1$ are periodic mod d.
(b) Show that there exist two integers in the range $0 \le r < s \le d$ for which $M_r \equiv M_s \pmod d$.
(c) In exercise 0.4.15(b) we saw that the Mersenne numbers satisfy the recurrence $M_{n+1} = 2M_n + 1$. Use this to show that $M_{r+j} \equiv M_{s+j} \pmod d$ for all $j \ge 0$.
(d) Deduce that there exists a positive integer $p = p_d$, which is $\le d$, such that $M_{n+p} \equiv M_n \pmod d$ for all $n \ge d$. That is, M_n is *eventually periodic* mod d with period $p_d \le d$.

Exercise 2.5.17. (a) By using the pigeonhole principle creatively, prove that there exist two integers in the range $0 \le r < s \le d^2$ for which $x_r \equiv x_s \pmod d$ *and* $x_{r+1} \equiv x_{s+1} \pmod d$.
(b) Use the recurrence for the x_n to show that $x_{r+j} \equiv x_{s+j} \pmod d$ for all $j \ge 0$.
(c) Deduce that the x_n are eventually periodic mod d with period $\le d^2$.
(d) Prove that m_d divides the period mod d.

Exercise 2.5.18. (a) Show that if there exists a positive integer r for which $x_r \equiv x_{r+1} \equiv 0 \pmod d$, then $x_n \equiv 0 \pmod d$ for all $n \ge r$ so that the x_n are eventually periodic mod d with period 1.
(b) Now assume that there does not exist a positive integer r for which $x_r \equiv x_{r+1} \equiv 0 \pmod d$. Modify the proof of exercise 2.5.17 to prove that the x_n are eventually periodic mod d with period $\le d^2 - 1$.

Exercise 2.5.19. In order to understand $x_n \pmod d$, we take $m = m_d$ in the results of this exercise.
(a) Prove, by induction, that $x_{m+k} \equiv x_{m+1}x_k \pmod{x_m}$ for all $k \geq 0$.
(b) Deduce the same result from exercise 0.4.10.
(c) Deduce that if $n = qm + r$ with $0 \leq r \leq m-1$, then $x_n \equiv (x_{m+1})^q x_r \pmod{x_m}$.

Exercise 2.5.20. Prove by induction that
(a) $x_{2k} \equiv ka(-b)^{k-1} \pmod\Delta$ and $x_{2k+1} \equiv (2k+1)(-b)^k \pmod\Delta$ for all $k \geq 0$ and
(b) $x_{2k} \equiv kab^{k-1} \pmod{a^2}$ and $x_{2k+1} \equiv b^k \pmod{a^2}$ for all $k \geq 0$.

Exercise 2.5.21. Suppose that the sequence $(u_n)_{n\geq 1}$ satisfies a dth-order linear recurrence (as defined in appendix 0B). Prove that for any integer $m > 1$, the u_n are eventually periodic mod m with period $\leq m^d - 1$. (We prove that this bound is best possible when m is prime in exercise 7.25.5.)

Appendix 2A. Congruences in the language of groups

2.6. Further discussion of the basic notion of congruence

2.7. Cosets of an additive group

Exercise 2.7.1. Prove that $a \equiv b \pmod m$ if and only if a/m and b/m belong to the same coset of $\mathbb{R}/\mathbb{Z}$.

Exercise 2.7.2. (a) Prove that $t \equiv \{t\} \pmod 1$ for all real numbers t.
(b) Prove that the usual rules of addition, subtraction, and multiplication hold mod 1.
(c) Show that division is not always well-defined mod 1, by finding a counterexample.

2.8. A new family of rings and fields

Exercise 2.8.1. Prove that $\mathbb{Z}/m\mathbb{Z}$ is a ring for all integers $m \geq 2$.

Exercise 2.8.2. (a) Prove that if m is a composite integer > 1, then $\mathbb{Z}/m\mathbb{Z}$ has zero divisors.
(b) Prove that $\mathbb{Z}/m\mathbb{Z}$ is not a field whenever m is a composite integer > 1.
(c) Prove that if R is any ring with zero divisors, then R cannot be a field.

2.9. The order of an element

Appendix 2B. The Euclidean algorithm for polynomials

2.10. The Euclidean algorithm in $\mathbb{C}[x]$

Exercise 2.10.1. Prove that if $a \in \mathbb{C}$, then $x - a$ is a factor of $f(x)$ if and only if $f(a) = 0$.

Exercise 2.10.2. Suppose the Euclidean algorithm gives the polynomials $F_0 = f, F_1 = g, F_2, F_3, \ldots$. Prove that, for all $k \geq 0$, there exist $a_k(x), b_k(x) \in \mathbb{C}[x]$ for which $F_k(x) = a_k(x)f(x) + b_k(x)g(x)$.

Exercise 2.10.3. (a) Show that A and B (with these degree bounds) are unique, up to a scalar multiple.
(b) Write $f = hF$ and $g = hG$ where $h = (f, g)$. Prove that all solutions of $a(x)f(x)+b(x)g(x) = h(x)$ are given by $a = A + kG$ and $b = B - kF$ for any $k(x) \in \mathbb{C}[x]$.

Exercise 2.10.4. Suppose that $f(x), g(x) \in \mathbb{Z}[x]$. Prove that $\gcd(f(x), g(x))_{\mathbb{C}[x]} = 1$ if and only if $\gcd(f(x), g(x))_{\mathbb{Q}[x]} = 1$.

Exercise 2.10.5. (a) Explain why the proof of Proposition 2.10.1 works in any field in place of $\mathbb{C}$.

(b) Prove that the result holds with $f(x), g(x) \in \mathbb{Z}[x]$, whenever g is monic.

(c) When $f(x), g(x) \in \mathbb{Z}[x]$ and $g(x)$ has leading coefficient $c \neq 0$, show that the result follows with "$f(x) = q(x)g(x) + r(x)$" replaced by "$c^{1+\deg f - \deg g} f(x) = q(x)g(x) + r(x)$".

2.11. Common factors over rings: Resultants and discriminants

2.12. Euclidean domains

Exercise 2.12.1. Prove that the Euclidean algorithm works in a Euclidean domain.

Exercise 2.12.2. Prove that $\mathbb{Z}[\omega]$ is a Euclidean domain, where $\omega = \frac{-1+\sqrt{-3}}{2}$.

Exercise 2.12.3. Suppose that R is a Euclidean domain (as defined above). Prove that for any $a, b \in R$ one can find $g \in R$ such that

- g divides both a and b using the Euclidean algorithm,
- there exists $u, v \in R$ for which $au + bv = g$, and
- if d also divides both a and b, then $w(d) \leq w(g)$.

We call g the greatest common divisor of a and b, measuring size using the function w.