CONSTRUCTION OF THE FINITE FIELDS $\mathbb{Z}_p$

S. R. DOTY

Elementary Number Theory

We begin with a bit of elementary number theory, which is concerned solely with questions about the set of integers $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$. We are not concerned with real numbers or fractions here.

We need the concept of divisibility in $\mathbb{Z}$, the division algorithm, and the Euclidean algorithm.

A.1. **Definition.** Let $a, b \in \mathbb{Z}$. Say that a *divides* b (written $a \mid b$) if there exists some $k \in \mathbb{Z}$ such that $b = ak$. We also say that b is *divisible* by a, or that b is a *multiple* of a, when this is so. If b is divisible by a, we also say that a is a *divisor* or *factor* of b.

Note that *any* integer divides 0.

A.2. **Lemma.** (Division Algorithm) Let m and n be given positive integers. There exist unique integers q, r such that

$$m = qn + r \qquad (0 \leq r < n).$$

The integers q, r are called the *quotient* and *remainder*, respectively. The procedure by which we obtain them is called long division, as you undoubtedly recall.

A.3. **Definition.** A positive integer $p > 1$ is *prime* if it has no positive integer divisors other than 1 and p.

Note that we explicitly exclude 1 from the set of prime numbers. The number 1 is *not* a prime! The primes in $\mathbb{Z}$ are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47 and so on. There are infinitely many primes in $\mathbb{Z}$.

A.4. **Definition.** Let $a, b \in \mathbb{Z}$. Any integer d such that $d \mid a$ and $d \mid b$ is called a *common divisor* of a, b. The *greatest common divisor* (gcd) of a, b is the largest of the common divisors. Write $\gcd(a, b)$ or more simply just (a, b) for the gcd of a, b.

Note that the gcd of the pair $0, 0$ is undefined, since there is no largest common divisor, but the gcd is well-defined in every other case. What is $\gcd(n, 0)$ when $n \neq 0$?

People say that a, b are *relatively prime* if their gcd is 1. This means that they have no prime factors in common, since if $p \mid a$ and $p \mid b$ then $(a, b) \geq p$ is surely larger than 1.

One way to compute the gcd of two given positive integers is to make a list of the divisors for each given number, and then the gcd is simply the largest number common to both lists. Of course, this is virtually impossible if the two numbers are large, but it works well enough for small numbers. For instance, let us compute the gcd of the pair $51, 33$ using this idea. The divisors of 49 are 1, 7, 49 and the divisors of 210 are 1, 2, 3, 5, 6, 7, 10, 14, 15, 21, 30, 42, 70, etc. The largest number that is common to both lists is 7, so $7 = \gcd(49, 210)$.

Another method is to factor each given number into its prime factorization. Although this is virtually impossible for very large numbers, it is pretty easy to do for small numbers. For instance, let us compute the gcd of the pair 209, 1368 using this idea. You can check with your calculator or by pen and paper that $209 = 11 \cdot 19$ and $1368 = 2^3 \cdot 3^2 \cdot 19$. Thus it follows immediately that $\gcd(209, 1368) = 19$. Note that this method, while better than the first method, still falls apart if we cannot find the prime factors of the numbers. (Please tell me the prime factors of 1273932017264838292093 if you doubt that this is a serious obstacle.)

A third way to compute the gcd is to use the *Euclidean algorithm*. It turns out that for large numbers this third way is far and away the best, in terms of efficiency. For instance, to compute the gcd of two random 100 digit numbers by a digital computer using the first or second method would require so many divisions that even the fastest computer would not compute an answer in a reasonable time. (It would take many years, even for the fastest supercomputer.) However, even a desktop PC could obtain an answer to the same problem using the Euclidean algorithm in a second or so, because only a few hundred divisions would be required! Now that you are convinced the Euclidean algorithm is a great thing for mankind, let's examine how it works.

A.5. **Euclidean algorithm.** Suppose you need to compute the gcd of integers a, b. For simplicity, assume both $a, b > 0$ and that a is the larger of the two. Repeatedly apply the division algorithm to get equations:

$$\begin{aligned} a &= bq + r && (0 \leq r < b) \\ b &= rq_1 + r_1 && (0 \leq r_1 < r) \\ r &= r_1 q_2 + r_2 && (0 \leq r_2 < r_1) \end{aligned}$$

$$r_1 = r_2 q_3 + r_3 \qquad (0 \le r_3 < r_2)$$

$$\vdots$$

The process terminates when you get a remainder of 0. The gcd of a, b is the last nonzero remainder in the above procedure.

The Euclidean algorithm, probably one of the first algorithms ever discovered, is the fastest known algorithm for computing the gcd of any two given numbers. It has a surprising number of applications to computer science, and is extremely useful in cryptography.

As an application of the Euclidean algorithm we have the following important result.

A.6. **Theorem.** Let $a, b \in \mathbb{Z}$, not both zero. There exist integers s, t such that $\gcd(a, b) = sa + tb$. (In other words, $\gcd(a, b)$ is expressible as an integral linear combination of a, b.)

Proof. The Euclidean algorithm equations can be worked backwards, with one substituted into another, until you reach this expression. To be specific, start with the last equation in which the remainder is nonzero. This can be rewritten to express that last nonzero remainder (the gcd) as a linear combination of the two remainders which precede it:

$$\gcd(a, b) = r_n = r_{n-2} - r_{n-1} q_n.$$

This is the base step, and it expresses $\gcd(a, b)$ as a linear combination of r_{n-1} and r_{n-2}.

Similarly, there is an equation which expresses r_{n-1} as a linear combination of the two remainders which precede it:

$$r_{n-1} = r_{n-3} - r_{n-2} q_{n-1}.$$

and putting that linear combination into the gcd equation above and grouping terms gives us

$$\begin{aligned} \gcd(a, b) &= r_{n-2} - (r_{n-3} - r_{n-2} q_{n-1}) q_n \\ &= (-q_n) r_{n-3} + (1 + q_{n-1} q_n) r_{n-2} \end{aligned}$$

which shows that $\gcd(a, b)$ is expressible as a linear combination of r_{n-2} and r_{n-3}.

One can repeat the process by induction until one arrives at a linear combination of a and b. □

A.7. **Example.** Here is an example which more clearly illustrates the proof of the previous theorem. Let's compute $\gcd(1521, 2004)$ using the Euclidean algorithm. Divide the bigger number by the smaller to get

$$2004 = 1 \cdot 1521 + 483. \tag{1}$$

Here the quotient is 1 and the remainder is 483. Now we divide 1521 by 483 to obtain

$$1521 = 3 \cdot 483 + 72. \tag{2}$$

Continuing, we divide 483 by 72 to obtain

$$483 = 6 \cdot 72 + 51. \tag{3}$$

Dividing 72 by 51 we obtain

$$72 = 1 \cdot 51 + 21. \tag{4}$$

Dividing 51 by 21 we obtain

$$51 = 2 \cdot 21 + 9. \tag{5}$$

Finally, dividing 21 by 9 we obtain

$$21 = 2 \cdot 9 + 3. \tag{6}$$

The process stops here because we will obtain a remainder of zero on the next division. This proves that $\gcd(1521, 2004) = 3$, which is the last nonzero remainder obtained by the process.

Now we work the equations backwards to express $\gcd(1521, 2004)$ as a linear combination of 1521 and 2004, as follows. By the last equation (6) we have, solving for the remainder:

$$3 = 21 - 2 \cdot 9.$$

Substitute $9 = 51 - 2 \cdot 21$, which comes from (5), to obtain

$$3 = 21 - 2(51 - 2 \cdot 21) = (-2)51 + (5)21;$$

substitute $21 = 72 - 51$, which comes from (4), to obtain

$$3 = (-2)51 + (5)(72 - 51) = (5)72 + (-7)51;$$

substitute $51 = 483 - 6 \cdot 72$, which comes from (3), to obtain

$$3 = (5)72 + (-7)(483 - 6 \cdot 72) = (-7)483 + (47)72;$$

substitute $72 = 1521 - 3 \cdot 483$, which comes from (2), to obtain

$$3 = (-7)483 + (47)(1521 - 3 \cdot 483) = (47)1521 + (-148)483;$$

substitute $483 = 2004 - 1521$, which comes from (1), to obtain

$$3 = (47)1521 + (-148)(2004 - 1521) = (-148)2004 + (195)1521.$$

This is the desired linear combination, since we have arrived at an expression $\gcd(1521, 2004) = 1521s+2004t$ with $s = 195$ and $t = -148$.

Now we apply the theorem to prove a fundamental fact about divisibility in the integers.

A.8. **Lemma.** (Euclid) If $a \mid (bc)$ and $\gcd(a, b) = 1$ then $a \mid c$.

Proof. By Theorem A.6, there exist integers s, t such that $1 = as + bt$. So $c = cas + cbt$. Since $a \mid bc$, both summands in the right-hand-side of the preceding equality are divisible by a. Thus c is divisible by a, as desired. □

A.9. **Definition.** Let $a, b \in \mathbb{Z}$. A *common multiple* of a, b is any integer m such that $a \mid m$, $b \mid m$. The *least common multiple* (lcm) of a, b is the smallest positive common multiple.

For example, $\operatorname{lcm}(5, 12) = 60$, $\operatorname{lcm}(16, 48) = 48$, and $\operatorname{lcm}(18, 99) = 198$. The relation between lcm and gcd is the following.

A.10. **Theorem.** Let $a, b \in \mathbb{Z}$. Then $\operatorname{lcm}(a, b) = ab/\gcd(a, b)$.

Proof. Try to find your own proof of this theorem, as a useful test of your understanding of divisibility. □

Modular Arithmetic

Next we come to the study of modular arithmetic and congruences. This is an important application of our brief study of number theory. Before giving the technical theory, it is perhaps worthwhile to make some comments on the intuition behind modular arithmetic.

The basic idea in modular arithmetic is embodied in the ordinary 12 hour clock. We all know that if it is currently 11 o'clock, then two hours from now will be 1 o'clock, because at 12 o'clock we start over again at zero. We can symbolize this situation by writing the equation $11 + 2 = 1 \pmod{12}$, or $11 + 2 \equiv 1 \pmod{12}$. (Either notation is common.)

To do modular arithmetic (that is, addition, subtraction, and multiplication) mod 12 we just compute as usual in $\mathbb{Z}$ taking into account that all multiples of 12 are the same as zero. Thus we have $10 + 5 \equiv 3 \pmod{12}$, $10 \cdot 5 \equiv 2 \pmod{12}$, and $5 - 10 \equiv -5 \equiv 7 \pmod{12}$. Note that the preferred answer for any modular arithmetic calculation is a natural number between 0 and 11 (inclusive). These are the same as the numbers on the face of the clock, except that 12 has been replaced by zero.

Modular arithmetic mod n (a positive integer) works exactly the same way, except that we replace the number 12 by the number n. Thus the preferred answer for a modular arithmetic calculation mod n is an integer in the closed interval $[0, n-1]$. Such integers are called *residues* mod n.

A.11. **Definition.** (Gauss) Let n be a given fixed positive integer. For $a, b \in \mathbb{Z}$ we say that a is *congruent* to b modulo n if n divides $a - b$. Write $a \equiv b \pmod{n}$ when this is so. Some folks write $a = b \pmod{n}$ instead.

A.12. **Theorem.** Congruence modulo n is an equivalence relation on the set $\mathbb{Z}$. That is:

(a) $a \equiv a \pmod{n}$ (reflexivity)
(b) $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$ (symmetry)
(c) $a \equiv b \pmod{n}$, $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$ (transitivity)
for all $a, b, c \in \mathbb{Z}$.

Proof. The proof is routine, and left for you to check. □

A.13. **Theorem.** Suppose that $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$. Then:

(a) $a + c \equiv b + d \pmod{n}$
(b) $ac \equiv bd \pmod{n}$.

Proof. Once again, the proof is a routine exercise. □

A.14. **Theorem.** If $\gcd(a, n) = 1$ then the congruence $ax \equiv b \pmod{n}$ is solvable, and its solution is uniquely determined modulo n.

Proof. (Existence) Since $\gcd(a, n) = 1$ we can find integers s, t such that $1 = as + nt$. Then $b = bas + bnt$. Thus $b \equiv abs \pmod{n}$. This proves that the integer $x = bs$ is a solution.

(Uniqueness) Suppose that we have two solutions x, x' to the given congruence. Then $ax \equiv b$ and $ax' \equiv b \pmod{n}$. Thus $ax \equiv ax' \pmod{n}$, so $n \mid (ax - ax')$, so $n \mid a(x - x')$. By Lemma A.8 we conclude that $n \mid (x - x')$, and so $x \equiv x' \pmod{n}$. □

It is important to notice that the proof not only shows that the congruence can be solved, but it actually tells us *how* to solve it, by means of the Euclidean algorithm. For instance, let us solve the congruence $121x \equiv 45 \pmod{390}$. By the Euclidean algorithm or otherwise, we find that $\gcd(121, 390) = 1$ and $1 = 9 \cdot 390 - 29 \cdot 121$. Multiplying by 45 as in the above proof we get that $45 = 9 \cdot 390 \cdot 45 - 29 \cdot 121 \cdot 45$,

so in other words $121(-29 \cdot 121) \equiv 45 \pmod{390}$. So a solution to $121x \equiv 45 \pmod{390}$ is given by $x = -29 \cdot 121) = -3509$. Since $x \equiv 389 \pmod{390}$ we can also use the simpler representative $x = 389$ to solve the congruence. (Any member of the equivalence class

$$E(-3509) = \{m \in \mathbb{Z} \mid m \equiv -3509 \pmod{390}\}$$

will solve the problem, and 389 is a member of this class as you can easily check.)

A.15. **Definition.** Any integer x such that $ax \equiv 1 \pmod{n}$ is called a *multiplicative inverse* of a modulo n. When such an x exists we say that a is *invertible* modulo n.

The preceding theorem says that whenever a is relatively prime to n then a is invertible modulo n. In fact, also conversely: if a is not relatively prime to n, then a is not invertible modulo n.

A.16. **Definition.** (The integers modulo n) Since congruence modulo n is an equivalence relation $\sim$ on the set $\mathbb{Z}$ of integers, it determines a partition of $\mathbb{Z}$ into disjoint equivalence classes. We write $\overline{a} = E(a)$ for the equivalence class containing an integer a. Thus

$$\overline{a} = \{b \in \mathbb{Z} \mid a \equiv b \pmod{n}\} = \{a + nk \mid k \in \mathbb{Z}\}.$$

Observe that an equivalence class simply collects together all the integers which leave the same remainder upon division by n.

Let $\mathbb{Z}_n = \mathbb{Z}/\sim$ be the set of equivalence classes mod n. We can define binary operations, "addition" and "multiplication," on the set $\mathbb{Z}_n$ as follows:

$$\overline{a} + \overline{b} = \overline{a + b}; \quad \overline{a}\,\overline{b} = \overline{ab}.$$

where on the right-hand-side of each equality we add or multiply as usual in $\mathbb{Z}$. This definition formalizes the intuition of modular arithmetic discussed previously. It may be verified that these binary operations are well-defined (i.e. independent of choice of representatives).

There are precisely n different equivalence classes in $\mathbb{Z}_n$. They correspond bijectively with the possible remainders (i.e., the residues) $\{0, 1, \ldots, n-1\}$ obtainable by division of an integer by n. Sometimes we use these numbers to denote the corresponding equivalence class.

EXAMPLE. Consider the integers mod 2. The equivalence classes mod 2 are the even and odd integers: $0 = \overline{0} = \{2n \mid n \in \mathbb{Z}\}$ and $1 = \overline{1} = \{2n + 1 \mid n \in \mathbb{Z}\}$. Mod 2 addition and multiplication can be

described in the following addition and multiplication tables

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

Mod 2 arithmetic is often called binary arithmetic. It is fundamental in digital computers and mathematical logic.

EXAMPLE. For another example, consider the integers mod 4. The equivalence classes mod 4 are the following:

$$0 = \overline{0} = \{4n \mid n \in \mathbb{Z}\}$$
$$1 = \overline{1} = \{4n+1 \mid n \in \mathbb{Z}\}$$
$$2 = \overline{2} = \{4n+2 \mid n \in \mathbb{Z}\}$$
$$3 = \overline{3} = \{4n+3 \mid n \in \mathbb{Z}\}.$$

Mod 4 addition and multiplication are summarized by the following addition and multiplication tables

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Commutative Rings and Number Fields

Next I want to introduce two useful formal algebraic structures. The definitions are based on axioms abstracted from familiar properties of ordinary integers and real numbers. We will obtain interesting examples of such structures from modular arithmetic. This was our main objective all along, and the reason we studied number theory and modular arithmetic.

A.17. **Definition.** Let A be a given set. A *binary operation* on the set A is a mapping $f : A \times A \to A$. Such a function has two arguments, that is, we have to write $f(x, y)$ to denote the function value. A binary operation combines two given elements of A to give another element of A.

Sometimes, if $*$ is a binary operation on a set A, we write $x * y$ instead of $*(x, y)$. For example, we always do that when $*$ is addition or multiplication, because writing $+(x, y)$ instead of the more familiar $x + y$ would look strange to us. Also, when $*$ is multiplication, we often abbreviate $x \cdot y$ to xy, as usual. It is important to realize that

although such conventions are adopted for convenience and comfort, nevertheless we still have a binary operation, no matter how we choose to write it.

A.18. **Definition.** A *commutative ring* is a set R with two binary operations, multiplication $\cdot$ and addition $+$, such that for all a, b, c in the set R we have:

(a) $a + b = b + a$; $ab = ba$ (commutativity)

(b) $a + (b + c) = (a + b) + c$; $a(bc) = (ab)c$ (associativity)

(c) $a(b + c) = ab + ac$ (distributivity);

moreover, there exist distinguished elements $0, 1$ in R such that

(d) $a + 0 = a$; $a1 = a$ for all a (identity);

and finally, for every $a \in R$, there exists some element $-a$ in R such that

(e) $a + (-a) = 0$ (additive inverse).

The element 0 is called the additive identity, while 1 is known as the multiplicative identity. The element $-a$ is the additive inverse of a, or the negative of a. We can subtract in a ring, because we can define $a - b = a + (-b)$. But division may not be possible in a ring. We can view a commutative ring as a set of objects along with a way to add, subtract, and multiply them, subject to the usual familiar properties of numbers.

EXAMPLES: The set of integers $\mathbb{Z}$ is a commutative ring under ordinary addition and multiplication. So are the sets of rational numbers $\mathbb{Q}$, real numbers $\mathbb{R}$, and complex numbers $\mathbb{C}$.

The set $\mathbb{Z}_n$ of equivalence classes mod n is a ring under modular addition and modular multiplication, as you can easily check. This ring is a *finite* ring since it contains just n different elements.

The set $\mathbb{N}$ of natural numbers under ordinary addition and multiplication is not a ring, because axiom (e) fails.

The ring $\mathbb{Z}_1$ of integers mod 1 is quite strange: it lumps together all of $\mathbb{Z}$ into just one equivalence class. We have just one element in this ring, so $0 = 1$ in this ring. This ring is sometimes called the zero ring or the trivial ring. It is not of much interest.

Here are some formal consequences of the definition, which must hold in any ring R, for all a, b, c in R:

(1) $a0 = 0$.

(2) $a(-b) = -(ab) = (-a)b$.

(3) $(-a)(-b) = ab$.

(4) $a(b-c) = ab - ac$.
(5) $(-1)a = -a$.

The proof of these basic facts is an exercise. For instance, to prove (a) one would begin with the equality $0 + 0 = 0$ (which comes from axiom (d) by taking $a = 0$ there), multiply both sides by a, and so forth.

A.19. **Definition.** An element a of a ring is said to be *invertible* if there is some b in the ring such that $ab = ba = 1$. If such an element b exists in the ring, we write $a^{-1} = b$. (Think of the inverse of a matrix.) An invertible element is also called a *unit* in the ring.

EXAMPLES. In $\mathbb{Z}_4$ the invertible elements are 1 and 3. In $\mathbb{Z}$ the invertible elements are 1 and -1. In the ring $\mathbb{R}$ of real numbers, every nonzero element is invertible.

A.20. **Definition.** A *field* is a commutative ring F in which $0 \neq 1$, and every nonzero element is invertible.

EXAMPLES: $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are all fields. The ring of integers $\mathbb{Z}$ is not a field.

Is the ring $\mathbb{Z}_n$ ever a field? The answer, which is provided by the following theorem, is quite satisfying.

A.21. **Theorem.** $\mathbb{Z}_n$ is a field if and only if n is prime.

Proof. This follows immediately from Theorem A.14. Suppose that n is prime. Let $a \neq 0$ in $\mathbb{Z}_n$. Then $\gcd(a, n) = 1$ since $a \in \{1, 2, \ldots, n-1\}$ and thus p cannot divide a. Hence there exists some $x \in \mathbb{Z}$ such that $ax \equiv 1 \pmod{n}$, so $\overline{x}$ is the inverse of a in $\mathbb{Z}_n$. This shows that $\mathbb{Z}_n$ is a field if n is prime.

On the other hand, if n is not prime then we can factor n in the form $n = ab$ for some integers $a, b < n$. Then a will not be invertible in $\mathbb{Z}_n$ since $ab = 0$ in $\mathbb{Z}_n$. (If you assume a is invertible then you can easily derive a contradiction from this.) □

NOTATION: In case $n = p$ is prime, it is customary to write $\mathbb{F}_p = \mathbb{Z}_p$ for this finite field of p elements.

Notice that the proof of the above theorem provides a procedure by which we can *compute* the inverse of an invertible element of $\mathbb{Z}_n$, by solving the corresponding congruence. Looking back at the proof of A.14 we see that to solve the congruence we can use the Euclidean algorithm. (For a small modulus, it is simpler to use trial and error since there are only finitely many possibilities to check.)

EXAMPLE. You can check that 7919 is prime. Let's compute the inverse of $a = 210$ in the finite field $\mathbb{Z}_{7919}$. The gcd of 210 and 7919 is 1, of course, and using the Euclidean algorithm we can find integers s and t such that $1 = 210s + 7919t$. In fact, $s = 1169$ and $t = -31$ as you can check. Thus $x = 1169$ is a solution to the congruence $210x \equiv 1 \pmod{7919}$, so the inverse of 210 in $\mathbb{Z}_{7919}$ is the element $210^{-1} = \overline{1169} = 1169$. You can check this by computing the residue of $210 \cdot 1169 \pmod{7919}$, which should be 1.

In any field, we can define division by any nonzero element b, by setting $a/b = ab^{-1}$. Intuitively, a field is a structure in which we have all the ordinary operations of arithmetic: addition, subtraction, multiplication, and division, such that these operations satisfy the usual properties of algebra. In addition to the familiar number fields $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ we have the novel finite fields $\mathbb{F}_p = \mathbb{Z}_p$ of p elements, for every prime number p.

Exercises

(1) (a) Use the Euclidean algorithm to compute $\gcd(48157656, 541541)$. (Use your calculator.)
(b) Find integers s, t such that
$$\gcd(48157656, 541541) = 48157656s + 541541t.$$
(2) Show that if $\gcd(a, n) \neq 1$ then a is not invertible modulo n.
(3) Compute the following:
(a) $2^{-1} \pmod 7$.
(b) $4^{-1} \pmod{15}$.
(c) $23^{-1} \pmod{275}$.
(d) $909^{-1} \pmod{81799}$. (Use Euclidean algorithm.)
(4) Use your answers to the preceding exercise to solve the congruences:
(a) $2x \equiv 4 \pmod 7$.
(b) $4x \equiv 13 \pmod{15}$.
(c) $23x \equiv 200 \pmod{275}$.
(d) $909x \equiv 8910 \pmod{81799}$.
Hint: Simply multiply by the inverse.
(5) Let R be a commutative ring. Prove, using only the axioms listed in the definition of commutative ring, that for any elements a, b, c of R we have:
(a) $a0 = 0$.
(b) $a(-b) = -(ab) = (-a)b$.
(c) $(-a)(-b) = ab$.
(d) $a(b - c) = ab - ac$.
(e) $(-1)a = -a$.
Note: $b - c = b + (-c)$ (definition).

(6) Show that the number of invertible elements in the ring $\mathbb{Z}_n$ is $\varphi(n)$, for any n. Here $\varphi(n)$ is the number of integers in the range $1, 2, \ldots, n$ which are relatively prime to n. The function φ is called *Euler's phi function*.
(7) Prove that congruence mod n is an equivalence relation on $\mathbb{Z}$ (Theorem A.12).
(8) Prove Theorem A.13.
(9) Show that a congruence $ax \equiv b \pmod{n}$ is solvable if and only if $\gcd(a, n)$ divides b.
(10) Explain the contradiction at the end of the proof of A.21. In other words, what is contradicted if you have elements $a \neq 0$, $b \neq 0$, and c in a ring such that $ac = 1$ and $ab = 0$?
(11) Prove Theorem A.10.