26

Modular Arithmetic

KARL FRIEDRICH GAUSS MADE the important discovery of modular arithmetic. Modular arithmetic is also called *clock arithmetic*, and we are actually used to doing modular arithmetic *all the time* (pun intended). For example, consider the question *If it is* 7 *o'clock now, what time will it be in* 8 *hours?*. Of course the answer is 3 o'clock, and we found the answer by adding $7 + 8 = 15$, and then subtracting 12 to get $15 - 12 = 3$. Actually, we are so accustomed to that sort of calculation, we probably just immediately blurt out the answer without stopping to think how we figured it out. But trying a less familiar version of the same sort of problem makes it plain exactly what we needed to do to answer such questions: *If it is* 7 *o'clock now, what time will it be in* 811 *hours?* To find out, we add $7 + 811 = 818$, then divide that by 12, getting $818 = (68)(12) + 2$, and so we conclude it will be 2 o'clock. The general rule is: to find the time h hours after t o'clock, add $h + t$, divide by 12 and take the remainder.

There is nothing special about the number 12 in the above discussion. We can imagine a clock with any integer number of hours (greater than 1) on the clock. For example, consider a clock with 5 hours. What time will it be 61 hours after 2 o'clock. Since $61 + 2 = 63 = (12)(5) + 3$, the answer is 3 o'clock.

In the general case, if we have a clock with m hours, then the time h hours after t o'clock will be the remainder when $t + h$ is divided by m.

26.1 The modulo m equivalence relation

This can all be expressed in more mathematical sounding language. The key is obviously the notion of remainder. That leads to the following definition:

So, the reason it is 2 o'clock 811 hours after 7 o'clock is that

$$811 + 7 \equiv 2 \pmod{12}$$

Definition 26.1. Given an integer $m > 1$, we say that two integers a and b are **congruent modulo** m, and write $a \equiv b \pmod{m}$, in case a and b leave the same remainder when divided by m.

Theorem 26.2. *Congruence modulo m defines an equivalence relation on* $\mathbb{Z}$.

Proof. *The relation is clearly reflexive since every number leaves the same remainder as itself when divided by m. Next, if a and b leave the same remainder when divided by m, so do b and a, so the relation is symmetric. Finally, if a and b leave the same remainder, and b and c leave the same remainder, then a and c leave the same remainder, and so the relation is transitive.* ♣

There is an alternative way to think of congruence modulo m.

Theorem 26.3. $a \equiv b \pmod{m}$ *if and only if* $m|(a-b)$.

Proof. *Suppose* $a \equiv b \pmod{m}$. *That means a and b leave the same remainder, say r when divided by m. So we can write* $a = jm + r$ *and* $b = km + r$. *Subtracting the second equation from the first gives* $a - b = (jm + r) - (km + r) = jm - km = (j-k)m$, *and that shows* $m|(a-b)$.

For the converse, suppose $m|(a-b)$. *Divide* a, b *by m to get quotients and remainders:* $a = jm + r$ *and* $b = km + s$, *where* $0 \le r, s < m$. *We need to show that* $r = s$. *Subtracting the second equation from the first gives* $a - b = m(j-k) + (r-s)$. *Since m divides* $a - b$ *and m divides* $m(j-k)$, *we can conclude m divides* $(a-b) - m(j-k) = r - s$. *Now since* $0 \le r, s < m$, *the quantity* $r - s$ *must be one of the numbers* $m-1, m-2, \cdots, 2, 1, 0, -1, -2, \cdots -(m-1)$. *The only number in that list that m divides is* 0, *and so* $r - s = 0$. *That is,* $r = s$, *as we wanted to show.* ♣

26.2 Equivalence classes modulo m

The equivalence class of an integer a with respect to congruence modulo m will be denoted by $[a]$, or $[a]_m$ in case we are employing more than one number m as a *modulus*. In other words, $[a]$ is the set of all integers that leave the same remainder as a when divided by m. Or, another way to say the same thing, $[a]$ comprises all integers b such that $b - a$ is a multiple of m. That means $b - a = km$, or $b = a + km$.

That last version is often the easiest way to think about the integers that appear in $[a]$: start with a and add and subtract any number of m's.

For example, the equivalence class of 7 modulo 11 would be

$$[7] = \{\cdots, -15, -4, 7, 18, 29, 40, \cdots\}.$$

We know that the distinct equivalence classes partition $\mathbb{Z}$. Since dividing an integer by m leaves one of $0, 1, 2, \cdots, m-1$ as a remainder, we can conclude that there are exactly m equivalence classes modulo m. In particular, $[0], [1], [2], [3], ...[m-1]$ is a list of all the different equivalence classes modulo m. It is traditional when working with modular arithmetic to drop the [ ] symbols denoting the equivalence classes, and simply write the representatives. So we would say, modulo m, there are m numbers: $0, 1, 2, 3, \cdots, m-1$. But keep in mind that each of those numbers really represents a set, and we can replace any number in that list with another equivalent to it modulo m. For example, we can replace the 0 by m. The list $1, 2, 3 \cdots, m-1, m$ still consists of all the distinct values modulo m.

26.3 Modular arithmetic

One reason the relation of congruence modulo m useful is that addition and multiplication of numbers modulo m acts in many ways just like arithmetic with ordinary integers.

Theorem 26.4. *If $a \equiv c \pmod{m}$, and $b \equiv d \pmod{m}$, then $a + b \equiv c + d \pmod{m}$ and $ab \equiv cd \pmod{m}$.*

Proof. *Suppose $a \equiv c \pmod{m}$ and $b \equiv d \pmod{m}$. Then there exist integers k and l with $a = c + km$ and $b = d + lm$. So $a + b = c + km + d + lm = (c + d) + (k + l)m$. This can be rewritten as $(a + b) - (c + d) =$*

$(k+l)m$, where $k+l \in \mathbb{Z}$. So $a+b \equiv c+d \pmod{m}$. The other part is done similarly. ♣

Example 26.5. *What is the remainder when $1103+112$ is divided by 11? We can answer this problem in two different ways. We could add 1103 and 112, and then divide by 11. Or, we could determine the remainders when each of 1103 and 112 is divided by 11, then add those remainders before dividing by 11. The last theorem promises us the two answers will be the same. In fact $1103+112 = 1215 = (110)(11)+5$ so that $1103+112 \equiv 5 \pmod{11}$. On the other hand $1103 = (100)(11)+3$ and $112 = (10)(11)+2$, so that $1103+112 \equiv 3+2 \equiv 5 \pmod{11}$.*

Example 26.6. *A little more impressive is the same sort of problem with operation of multiplication: what is the remainder when $(1103)(112)$ is divided by 11? The calculation looks like $(1103)(112) \equiv (3)(2) \equiv 6 \pmod{11}$.*

Example 26.7. *For a really awe inspiring example, let's find the remainder when 1103^{112} is divided by 11. In other words, we want to find $x = 0,1,2,\cdots 10$ so that $1103^{112} \equiv x \pmod{11}$.*

Now 1103^{112} is a pretty big number (in fact, since $\log 1103^{112} = 112\log 1103 = 340.7\cdots$, the number has 341 digits). In order to solve this problem, let's start by thinking small: Let's compute 1103^n, for $n = 1,2,3,\cdots$.

$$\begin{aligned}
1103^1 &\equiv 1103 \equiv 3 \pmod{11}\\
1103^2 &\equiv 3^2 \equiv 9 \pmod{11}\\
1103^3 &\equiv 1103(1103^2) \equiv 3(9) \equiv 27 \equiv 5 \pmod{11}\\
1103^4 &\equiv (1103)(1103^3) \equiv 3(5) \equiv 15 \equiv 4 \pmod{11}\\
1103^5 &\equiv (1103)(1103^4) \equiv 3(4) \equiv 12 \equiv 1 \pmod{11}
\end{aligned}$$

Now that last equation is very interesting. It says that whenever we see 1103^5 we may just as well write 1 if we are working modulo 11. And now we see there is an easy way to determine 1103^{112} modulo 11:

$$1103^{112} \equiv 1103^{5(22)+2} \equiv (1103^5)^{22}(1103^2) \equiv 1^{22}(9) \equiv 9 \pmod{11}$$

The sort of computation in example 26.7 appears to be just a curiosity, but in fact the last sort of example forms the basis of one version of public key cryptography. Computations of exactly that type (but with much larger integers) are made whenever you log into a secure Internet site. It's reasonable to say that e-commerce owes its existence to the last theorem.

While modular arithmetic in many ways behaves like ordinary arithmetic, there are some differences to watch for. One important difference is the familiar *rule of cancellation*: in ordinary arithmetic, if $ab = ac$ and $a \neq 0$, then $b = c$. This rule fails in modular arithmetic. For example, $3 \not\equiv 0 \pmod 6$ and $(3)(5) \equiv (3)(7) \pmod 6$, but $5 \not\equiv 7 \pmod 6$.

26.4 *Solving congruence equations*

Solving congruence equations is a popular sport. Just as with regular arithmetic with integers, if we want to solve $a + x \equiv b \pmod m$, we can simply set $x \equiv b - a \pmod m$. So, for example, solving $55 + x \equiv 11 \pmod 6$ we would get $x \equiv 11 - 55 \equiv -44 \equiv 4 \pmod 6$.

Equations involving multiplication, such as $ax \equiv b \pmod m$, are much more interesting. If the modulus m is small, equations of this sort can be solved by trial-and-error: simply try all possible choices for x. For example, testing $x = 0, 1, 2, 3, 4, 5, 6$ in the equation $4x \equiv 5 \pmod 7$, we see $x \equiv 3 \pmod 7$ is the only solution. The equation $4x \equiv 5 \pmod 8$ has no solutions at all. And the equation $2x \equiv 4 \pmod 6$ has $x \equiv 2, 5 \pmod 6$ for solutions.

Trial-and-error is not a suitable approach for large values of m. There is a method that will produce all solutions to $ax \equiv b \pmod m$. It turns out that such equations are really just linear Diophantine equations in disguise, and that is the key to the proof of the following theorem.

Theorem 26.8. *The congruence $ax \equiv b \pmod m$ can be solved for x if and only if $d = \gcd(a, m)$ divides b.*

This is why $4x \equiv 5 \pmod 7$ has a solution: $gcd(4,7) = 1$ and $1|5$. And, why $4x \equiv 5 \pmod 8$ has no solutions: $gcd(4,8) = 4$, but $4 \not| 5$.

Proof. *Solving $ax \equiv b \pmod m$ is the same as finding x so that $m|(ax - b)$ and that's the same as finding x and y so that $ax - b = my$.*

Rewriting that last equation in the form $ax + (-m)y = b$, we can see solving $ax \equiv b \pmod{m}$ is the same as solving the linear Diophantine equation $ax + (-m)y = b$. We know that equation has a solution if and only if $gcd(a, m)|b$, so that proves the theorem. ♣

The theorem also shows that $2x \equiv 4 \pmod{6}$ has a solution since $gcd(2, 6) = 2$ and $2|4$. But why does this last equation have two solutions? The answer to that is also provided by the results concerning linear Diophantine equations.

Let $\gcd(a, m) = d$. The solutions to $ax \equiv b \pmod{m}$ are the same as the solutions for x to $ax + (-m)y = b$. Supposing that last equation has a solution with $x = s$, then we know all possible choices of x are given by $x = s + k\frac{m}{d}$. So if $x = s$ is one solution to $ax \equiv b \pmod{m}$, then all solutions are given by $x = s + k\frac{m}{d}$, where k is any integer. In other words, all solutions are given by $x \equiv s \pmod{\frac{m}{d}}$, and so there are d solutions modulo m,

Example 26.9. *Let's find all the solutions to $2x \equiv 4 \pmod{6}$. Since $x = 2$ is obviously one solution, we see all solutions are given by $x = 2 + k\frac{6}{2} = 2 + 3k$, where k is any integer. When $k = 0, 1$ we get $x = 2, 5$, and other values of k repeat these two modulo 6. Looking at the solutions written as $x = 2 + k\frac{6}{2} = 2 + 3k$, we can see another way to express the solutions would be as $x \equiv 2 \pmod{3}$.*

Example 26.10. *Find all solutions to $42x \equiv 35 \pmod{91}$.*

Using the continued fraction method (or just staring at the numbers 42 and 91 long enough) we see $gcd(91, 42) = 7$ and, since $7|35$, the equation will have a solution. In fact, since $gcd(42, 91) = 7$, there are going to be seven solutions modulo 91. All we need is to find one particular solution, then the others will all be easy to determine. Again using the continued fraction method (or just playing with 42 and 91 a little bit) we discover $(42)(-2) + (91)(1) = 7 = gcd(42, 91)$. Multiplying by 5 gives $(42)(-10) + (91)(5) = 35$. The only thing we care about is that $x = -10$ is one solution to $42x \equiv 35 \pmod{91}$. As above, it follows that all solutions are given by $x \equiv -10 \pmod{)}\frac{91}{gcd(42,91)}$. That's the same as $x \equiv -10 \pmod{13}$, or, even more neatly, $x \equiv 3 \pmod{13}$. In other words, the solutions are $3, 16, 29, 42, 55, 68, 81$ modulo 91.

26.5 Exercises

Exercise 26.1.

(a) *On a military (24-hour) clock, what time is it* 3122 *hours after* 16 *hundred hours?*

(b) *What day of the week is it* 3122 *days after a Monday?*

(c) *What month is it* 3122 *months after November?*

Exercise 26.2. *List the integers in* $[7]_{11}$.

Exercise 26.3. *In a listing of the five equivalence classes modulo* 5*, four of the values are* 1211, 218, -100*, and* -3333*. What are the possible choices for the fifth value?*

Exercise 26.4. *Determine* n *between* 0 *and* 24 *such that*
$2311 + 3912 \equiv n \pmod{25}$.

Exercise 26.5. *Determine* n *between* 0 *and* 24 *such that*
$(2311)(3912) \equiv n \pmod{25}$.

Exercise 26.6. *Determine* n *between* 0 *and* 8 *such that*
$1111^{2222} \equiv n \pmod{9}$.

Exercise 26.7. *Solve:* $4x \equiv 3 \pmod{7}$.

Exercise 26.8. *Solve* $11x \equiv 8 \pmod{57}$.

Exercise 26.9. *Solve:* $14x \equiv 3 \pmod{231}$.

Exercise 26.10. *Solve* $8x \equiv 16 \pmod{28}$

Exercise 26.11. *Solve:* $91x \equiv 189 \pmod{231}$

Exercise 26.12. *Let* $d = gcd(a, m)$*, and let* s *be a solution to* $ax \equiv b \pmod{m}$.

(a) *Show that if* $ax \equiv b \pmod{m}$*, then there is an integer* r *such that* $x = s + r\left(\frac{m}{d}\right)$.

(b) *If* $0 \leq r_1 < r_2 < d$*, then the numbers* $x_1 = s + r_1\left(\frac{m}{d}\right)$ *and* $x_2 = s + r_2\left(\frac{m}{d}\right)$ *are not congruent modulo* m.

26.6 Problems

Problem 26.1. *Suppose we have a* 52 *card deck with the cards in order, top to bottom, ace* $, 2, 3, \ldots,$ *queen, king for clubs, then diamonds, then hearts, then spades. A step consists to taking the top card and moving it to the bottom of the deck. We start with the ace of clubs as the top card. After two steps, the top card is the* 3 *of clubs. What is the top card after* 735 *steps?*

Problem 26.2. *The marks on a combination lock are numbered* 0 *to* 39*. If the lock is at mark* 19*, and the dial is turned one mark clockwise, it will be at mark* 18*. If the lock is at mark* 19 *and turned* 137 *marks clockwise, at what mark will it be?*

Problem 26.3. *List the integers in* $[11]_7$*.*

Problem 26.4. *Arrange the numbers* $-39, -27, -8, 11, 37, 68, 91$ *so they are in the order* $0, 1, 2, 3, 4, 5, 6$ *modulo* 7*.*

Problem 26.5. *Determine* n *between* 0 *and* 16 *such that* $311 + 891 \equiv n \pmod{17}$*.*

Problem 26.6. *Determine* n *between* 0 *and* 16 *such that* $(405)(777) \equiv n \pmod{17}$*.*

Problem 26.7. *Determine* n *between* 0 *and* 16 *such that* $710^{447} \equiv n \pmod{17}$*.*

Problem 26.8. *Solve:* $3x \equiv 5 \pmod{8}$*.*

Problem 26.9. *Solve:* $13x \equiv 12 \pmod{68}$*.*

Problem 26.10. *Solve:* $15x \equiv 12 \pmod{27}$*.*

Problem 26.11. *Solve:* $12x \equiv 9 \pmod{88}$*.*

Problem 26.12. *Solve:* $33x \equiv 183 \pmod{753}$*.*

Problem 26.13. *There is exactly one* n *between* 0 *and* 55 *such that* $n \equiv 6 \pmod{7}$ *and* $n \equiv 1 \pmod{8}$*. Determine that* n*.*

Problem 26.14. *There is exactly one* n *between* 0 *and* 19548 *such that* $n \equiv 22 \pmod{173}$ *and* $n \equiv 80 \pmod{113}$*. Determine that* n*.*

28

The Two Fundamental Counting Principles

THE NEXT FEW CHAPTERS WILL DEAL with the topic of **combinatorics:** the art of counting. By counting we mean determining the number of different ways of arranging objects in certain patterns or the number of ways of carrying out a sequence of tasks. For example, suppose we want to count the number of ways of making a bit string of length two. Such a problem is small enough that the possible arrangements can be counted by *brute force*. In other words, we can simply make a list of all the possibilities: $00, 01, 10, 11$. So the answer is four. If the problem were to determine the number of bit strings of length fifty, the brute force method loses a lot of its appeal. For problems where brute force counting is not a reasonable alternative, there are a few principles we can apply to aid in the counting. In fact, there are just two basic principles on which all counting ultimately rests.

Throughout this chapter, all sets mentioned will be finite sets, and if A is a set, $|A|$ will denote the number of elements in A.

28.1 The sum rule

The **sum rule** says that if the sets A and B are disjoint, then

$$|A \cup B| = |A| + |B|.$$

Example 28.1. *For example, if $A = \{a, b, c\}$ and $B = \{j, k, l, m, n\}$, then $|A| = 3, |B| = 5$, and, sure enough,*

$$|A \cup B| = |\{a, b, c, j, k, l, m, n\}| = 8 = 3 + 5.$$

Care must be used when applying the sum principle that the sets are disjoint. If $A = \{a, b, c\}$ and $B = \{b, c, d\}$, then $|A \cup B| = 4$, and not 6.

Example 28.2. *As another example of the sum principle, if we have a collection of* 3 *dogs and* 5 *cats, then we can select one of the animals in* 8 *ways.*

28.1.1 Counting two independent tasks

The sum principle is often expressed in different language: If we can do task 1 in m ways and task 2 in n ways, and the tasks are *independent* (meaning that both tasks cannot be done at the same time), then there are $m + n$ ways to do one of the two tasks. The independence of the tasks is the analog of the disjointness of the sets in the set version of the sum rule.

A serious type of error is trying to use the sum rule for tasks that are not independent. For instance, suppose we want to know *in how many different ways we can select either a deuce or a six from an ordinary deck of* 52 *cards.* We could let the first task be the process of selecting a deuce from the deck. That task can be done in 4 ways since there are 4 deuces in the deck. For the second task, we will take the operation of selecting a six from the deck. Again, there are 4 ways to accomplish that task. Now these tasks are independent since we cannot simultaneously pick a deuce and a six from the deck. So, according to the sum rule, there are $4 + 4 = 8$ ways of selecting one card from a deck, and having that card be either a deuce or a six.

Now consider the similar sounding question: *In how many ways can we select either a deuce or a diamond from a deck of* 52 *cards?* We could let the first task again be the operation of selecting a deuce from the deck, with 4 ways to carry out that task. And we could let the second task be the operation of selecting a diamond from the deck, with 13 ways to accomplish that. But in this case, the answer to the question is not $4 + 13 = 17$, since these tasks are not independent. It is possible to select a card that is both a deuce and a diamond. So the sum rule cannot be used. What is the correct answer? Well, there are 13 diamonds, and there are 3 deuces besides the two of diamonds, and so there are actually 16 cards in the deck that are either a deuce or a diamond. That means there are 16 ways to select a card from a deck and have it turn out to be either a deuce or a diamond.

28.1.2 Extended sum rule

The sum rule can be extended to the case of more than two sets (or more than two tasks): If $A_1, A_2, A_3, \cdots, A_n$ is a collection of *pairwise disjoint* sets, then $|A_1 \cup A_2 \cup A_3 \cup \cdots \cup A_n| = |A_1| + |A_2| + |A_3| + \cdots + |A_n|$. Or, in terms of tasks: If task 1 can be done in k_1 ways, and task 2 in k_2, and task 3 in k_3 ways, and so on, until task n can be done in k_n ways, and if the tasks are all independent[1], then we can do one task in $k_1 + k_2 + k_3 + \cdots + k_n$ ways.

Example 28.3. *For example, if we own three cars, two bikes, a motorcycle, four pairs of roller skates, and two scooters, then we can select one of these modes of transportation in* $3 + 2 + 1 + 4 + 2 = 12$ *ways.*

28.1.3 Sum rule and the logical or

The sum rule is related to the logical connective *or*. That is reasonable since the sum rule counts the number of elements in the set $A \cup B = \{ x \mid x \in A \text{ or } x \in B \}$. In terms of tasks, the sum rule counts the number of ways to do either task 1 or task 2. Generally speaking, when the word *or* occurs in a counting problem, the sum rule is the tool to use.

But, verify independence!

28.2 The product rule

The logical connective *and* is related to the second fundamental counting principle: the **product rule**. The product rule says:

$$|A \times B| = |A| \cdot |B|.$$

[1] They must be **pairwise** independent!

An explanation of this is that $A \times B$ consists of all ordered pairs (a, b) where $a \in A$ and $b \in B$. There are $|A|$ choices for a and then $|B|$ choices for b.

28.2.1 Counting two sequential tasks: logical and

In terms of tasks, the product rule says that if task 1 can be done in m ways and task 2 can be done in n ways after task 1 has been done, then there are mn ways to do both tasks, the first then the second. Here the relation with the logical connective *and* is also obvious. We need to do task 1 and task 2. Generally speaking, the appearance of *and* in a counting problem suggests the product rule will come into play.

28.2.2 Extended product rule

As with the sum rule, the product rule can be used for situations with more than two sets or more than two tasks. In terms of sets, the product rule reads $|A_1 \times A_2 \times \cdots A_n| = |A_1| \cdot |A_2| \cdots |A_n|$. In terms of tasks, it reads, if task 1 can be done in k_1 ways, and for each of those ways, task 2 can be done in k_2 ways, and for each of those ways, task 3 can be done in k_3 ways, and so on, until for each of those ways, task n can be done in k_n ways, then we can do task 1 followed by task 2 followed by task 3, etc, followed by task n in $k_1 k_2 k_3 \cdots k_n$ ways. That sounds worse than it really is.

Example 28.4. *How many bit strings are there of length five?*

Solution. *We can think of task* 1 *as filling in the first (right hand) position, task* 2 *as filling in the second position, and so on. We can argue that we have two ways to do task* 1*, and then two ways to do task* 2*, and then two ways to do task* 3*, and then two ways to do task* 4*, and then two ways to do task* 5*. So, by the product rule, there are* $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^5 = 32$ *ways to do all five tasks, and so there are* 32 *bit strings of length five.*

The same reasoning shows that, in general, there are 2^n bit strings of length n.

Example 28.5. *Suppose we are buying a car with five choices for the exterior color and three choices for the interior color. Then there is a total of* $3 \cdot 5 = 15$ *possible color combinations that we can choose from. The first task is to select an exterior color, and there are* 5 *ways to do that. The second task* *is to select an interior color, and there are* 3 *ways to do that. So the product rule says there are* 15 *ways total to do both tasks. Notice that there is no requirement of independence of tasks when using the product rule. However, also notice that the number of ways of doing the second task* ***must*** *be the same no matter what choice is made for doing the first task.*

Example 28.6. *For another, slightly more complicated, example of the product rule in action, suppose we wanted to make a two-digit number using the digits* 1, 2, 3, 4, 5, 6, 7, 8, *and* 9*. How many different such two-digit numbers could we form? Let's make the first task filling in the left digit, and the second task filling in the right digit. There are* 9 *ways to do the first task. And, no matter how we do the first task, there are* 9 *ways to do the second task as well. So, by the product rule, there are* $9 \cdot 9 = 81$ *possible such two-digit numbers.*

Example 28.7. *Now, let's change the problem in example 28.6 a little bit. Suppose we wanted two-digit numbers made up of those same nine digits, but we do not want to use a digit more than once in any of the numbers. In other words,* 37 *and* 91 *are OK, but we do not want to count* 44 *as a possibility. We can still make the first task filling in the left digit, and the second task filling in the right digit. And, as before, there are* 9 *ways to do the first task. But now, once the first task has been done, there are only* 8 *ways to do the second task, since the digit used in the first task is no longer available for doing the second task. For instance, if the digit* 3 *was selected in the first task, then for the second task, we will have to choose from the eight digits* 1, 2, 4, 5, 6, 7, 8, *and* 9*. So, according to the product rule, there are* $9 \cdot 8 = 72$ *ways of building such a number.*

No matter in what way the first task was done, there are always 8 ways to to the second task in sequence. What if you chose to pick the second digit first?

Example 28.8. *Just for fun, here is another way to see the answer in example 28.7 is* 72*. We saw above that there are* 81 *ways to make a two-digit number when we allow repeated digits. But there are* 9 *two digit numbers that do have repeated digits (namely* $11, 22, \cdots, 99$*). That means there must be* $81 - 9 = 72$ *two-digit numbers without repeated digits.*

28.2.3 Counting by subtraction: Good = Total − Bad

The trick we used in example 28.8 looks like a new counting principle, but it is really the sum rule being applied in a tricky way. Here's the idea. Call the set of all the two-digit numbers (not using 0) T, call the set with no repeated digits N, and call the set with repeated digits R. By the sum rule, $|T| = |N| + |R|$, so $|N| = |T| - |R|$. This is a very common trick.

Generally, suppose we are interested in counting some arrangements, let's call them the *Good* arrangements. But it is not easy for some reason to count the *Good* arrangements directly. So, instead, we count the *Total* number of arrangements, and subtract the number of *Bad* arrangements:

$$\mathit{Good} = \mathit{Total} - \mathit{Bad}.$$

Let's have another example of this trick.

Example 28.9. *By a word of length five, we will mean any string of five letters from the* 26 *letter alphabet. How many words contain at least one vowel. The vowels are:* a,e,i,o,u.

By the product rule, there is a total of 26^5 *possible words of length five. The bad words are made up of only the* 21 *non-vowels. So, by the sum rule, the number of good words is* $26^5 - 21^5$.

28.3 Using both the sum and product rules

As in example 28.9, most interesting counting problems involve a combination of both the sum and product rules.

Example 28.10. *Suppose we wanted to count the number of different possible bit strings of length five that start with either three* 0*'s or with two* 1*'s. Recall that a bit string is a list of* 0*'s and* 1*'s, and the length of the bit string is the total number of* 0*'s and* 1*'s in the list. So, here are some bit strings that satisfy the stated conditions:* 00001, 11111, 11011, *and* 00010. *On the other hand, the bit strings* 00110 *and* 10101 *do not meet the required condition.*

To do this problem, let's first count the number of good bit strings that start with three 0*'s. In this case, we can think of the construction of such a bit string as doing five tasks, one after the other, filling in the leftmost bit, then the next one, then the third, the next, and finally the last bit. There is only one way to do the first three tasks, since we need to fill in* 0*'s in the first three positions. But there are two ways to do the last two tasks, and* *so, according to the product rule there are* $1 \cdot 1 \cdot 1 \cdot 2 \cdot 2 = 4$ *bit strings of length five starting with three* 0*'s. Using the same reasoning, there are* $1 \cdot 1 \cdot 2 \cdot 2 \cdot 2 = 8$ *bit strings of length five starting with two* 1*'s. Now, a bit string cannot both start with three* 0*'s and also with two* 1*'s, (in other words, starting with three* 0*'s and starting with two* 1*'s are independent). And so, according to the sum rule, there will be a total of* $4 + 8 = 12$ *bit strings of length five starting with either three* 0*'s or two* 1*'s.*

Example 28.11. *How many words of six letters (repeats OK) contain exactly one vowel?*

Solution. *Let's break the construction of a good word down into a number of tasks.*

Task 1: Select a spot for the vowel: 6 *choices.*

Task 2: Select a vowel for that spot: 5 *choices.*

Task 3: Fill first empty spot with a non-vowel: 21 *choices*

Task 4: Fill next empty spot with a non-vowel: 21 *choices*

Task 5: Fill next empty spot with a non-vowel: 21 *choices*

Task 6: Fill next empty spot with a non-vowel: 21 *choices*

Task 7: Fill last empty spot with a non-vowel: 21 *choices*

By the product rule, the number of good words is $6 \cdot 5 \cdot 21^5$.

Example 28.12. *Count the number of strings on license plates which either consist of three capital English letters, followed by three digits, or consist of two digits followed by four capital English letters.*

Solution. *Let* A *be the set of strings which consist of three capital English letters followed by three digits, and* B *be the set of strings which consist of two digits followed by four capital English letters. By the product rule* $|A| = 26^3 \cdot 10^3$ *since there are 26 capital English letters and 10 digits. Also by the product rule* $|B| = 10^2 \cdot 26^4$*. Since* $A \cap B = \emptyset$*, by the sum rule the answer is* $26^3 \cdot 10^3 + 10^2 \cdot 26^4$.

28.4 *Answer form $\longleftrightarrow$ solution method*

In the previous examples we might continue on with the arithmetic. For instance, in the last, example 28.12, using the distributive law on our answer to factor out common terms we see $|A \cup B| = 10^2 \cdot 26^3(10 + 26)$ is an equivalent answer. This, in turn, simplifies to $|A \cup B| = 10^2 \cdot 26^3 \cdot 36$, and that gives

$$|A \cup B| = 100 \cdot 17576 \cdot 36 = 63,273,600.$$

Of all of these answers the most valuable is probably $26^3 \cdot 10^3 + 10^2 \cdot 26^4$, since **the form of the answer is indicative of the manner of solution.** We can readily observe that the sum rule was applied to two disjoint subcases. For each subcase the product rule was applied to compute the intermediate answer. As a general rule, answers to counting problems should be left in this uncomputed form.

The next most useful solution is the last one. When we have an answer of this form we can use it to consider whether or not our answer makes sense intuitively. For example if we knew that A and B both were subsets of a set of cardinality 450 and we computed that $|A \cup B| > 450$, this would indicate that we made an error, either in the logic of our counting, or in arithmetic, or both.

28.5 Exercises

Exercise 28.1. *To meet the science requirement a student must take one of the following courses: a choice of* 5 *biology courses,* 4 *physics courses, or* 6 *chemistry courses. In how many ways can the one course be selected?*

Exercise 28.2. *Using the data of problem 1, a student has decided to take one biology, one physics, and one chemistry course. How many different such selections are possible?*

Exercise 28.3. *A serial code is formed in one of three ways: (1) two letters followed by two digits, or (2) three letters followed by one digit, or (3) four letters. How many different codes are there? (Unless otherwise indicated, letters will means upper case letters chosen from the usual* 26*-letter alphabet and digits are selected from* $\{0,1,2,3,4,5,6,7,8,9\}$*.)*

Exercise 28.4. *How many words of length six are there if letters may be repeated? (Examples: BBBXBB, ABATBC are OK).*

Exercise 28.5. *How many words of length six are there if letters may not be repeated? (Examples: BBBBXB, ABATJC are bad but ABXHYR is OK).*

Exercise 28.6. *A true/false test contains 25 questions.*

(a) *How many ways can a student complete the test if every question must be answered?*

(b) *How many ways can a student complete the test if questions can be left unanswered?*

Exercise 28.7. *How many binary strings of length less than or equal to nine are there?*

Exercise 28.8. *How many eight-letter words contain at least one A?*

Exercise 28.9. *How many seven-letter words contain at most one A?*

Exercise 28.10. *How many nine-letter words contain at least two A's?*

28.6 Problems

Problem 28.1. *My piggy bank contains* 20 *pennies,* 4 *nickels,* 7 *dimes, and* 2 *quarters. In how many ways can I select one coin?*

Problem 28.2. *My piggy bank contains* 20 *pennies,* 4 *nickels,* 7 *dimes, and* 2 *quarters. In how many ways can I select four coins, one of each value?*

Problem 28.3. *A multiple choice test contains 10 questions. There are four possible answers for each question.*

(a) *How many ways can a student complete the test if every question must be answered?*

(b) *How many ways can a student complete the test if questions can be left unanswered?*

Problem 28.4. *Computer ID's are length seven strings made up of any combination of seven different letters and digits. How many different ID's are there?*

Problem 28.5. *Computer ID's are length seven strings made up of any combination of seven letters and digits, with repeats allowed. How many different ID's are there?*

Problem 28.6. *A code word is either a sequence of three letters followed by two digits or two letters followed by three digits. (Unless otherwise indicated, letters will means upper case letters chosen from the usual* 26*-letter alphabet and digits are selected from* $\{0,1,2,3,4,5,6,7,8,9\}$*.) How many different code words are possible?*

Problem 28.7. *Code words consist of five letters followed by five digits. How many code word contain at least one X?*

Problem 28.8. *Code words consist of five letters followed by five digits. How many code word contain exactly one X?*

Problem 28.9. *Code words consist of five letters followed by five digits. How many code word contain exactly two X's?*

Problem 28.10. *How many bit strings of length ten begin and end with* 1*'s?*

Problem 28.11. *How many bit strings of length t least two but no more than ten begin and end with* 1*'s?*

Problem 28.12. *There are five roads from A to B, three roads from B to C, and five roads from C to D. How many different routes are there from A to B to C to D?*

Problem 28.13. *There are five roads from A to B, three roads from B to C, and five roads from C to D. How many different round trip routes are there from A to D and back to A?*

Problem 28.14. *There are five roads from A to B, three roads from B to C, and five roads from C to D. How many different round trip routes are there from A to D and back to A if you cannot travel over any road more than once?*