12

Card Dealing

and

The Chinese Remainder Theorem

Many classroom exercises involve dealing cards. In this chapter we will focus on a simple problem: Write an algorithm to *randomly* select one card out of an ordinary 52-card deck. My students frequently derive an efficient algorithm to solve this problem. The algorithm goes as follows we use a random number generator to select a number between 1 and 52 (or between 0 and 51; either way works fine). Given this number, for example 35, we need a method of assigning the number a suit and a value. This method must assign a unique card to each number. The method usually employed works as follows: Compute the number mod 4. In our example 35 mod 4 is 3. We consider 3 as spades (0 is clubs, 1 is diamonds, and 2 is hearts). Next compute the number mod 13. In this example 35 mod 13 is 9. This corresponds to the value 10 (0 is an ace, 1 is a deuce, 2 is a 3, up to 12 which is a king). Hence our card is the 10 of Spades. There is nothing at all wrong with the above algorithm. However, suppose we had a deck of 40 cards, with four suits and values from Ace to 10. Now the choosing a value between 1 and 40 we compute the number mod 4 and mod 10. This means that 15 and 35 each correspond to 6 of Spades. Our algorithm works in one case but not the other.

The first case worked because 4 and 13 are relatively prime, $4 \perp 13$. Similarly, in the second case 4 and 10 are **not** relatively prime. This can be made precise by the Chinese remainder theorem. However, first we need to take care of an issue:

Theorem: Suppose $x_1, x_2, ..., x_n$ are pairwise relatively prime. (That is $i \neq j$ implies $x_i \perp x_j$.) Then $x_1 \perp x_2 \cdot x_3 \cdot x_4 \cdot ... \cdot x_n$. (In other words, any number in the set is relatively prime to the product of the others.)

Proof: Suppose otherwise; then there is some prime p such that $p|x_1$ and $p|x_2 \cdot x_3 \cdot x_4 \cdot ... \cdot x_n$. Now if p does not divide x_i for some i then $p \perp x_i$, since p is a prime. Hence if p does not divide x_2 then by Euclid's Lemma $p|x_3 \cdot x_4 \cdot ... \cdot x_n$. In the latter case, we can peel off x_3 just as we did x_2 and we can continue like this until $p|x_k$ for some k. We know that there must be some such k since the process cannot continue indefinitely. Since p divides both x_1 and x_k, it is not true that $x_1 \perp x_k$. Thus we have contradicted one of our assumptions and the theorem is proven.

The utility of this theorem will be explained at the end of the next example.

The Chinese Remainder Theorem

Suppose we have the system of equations:

$x \equiv c_1 \bmod m_1$
$x \equiv c_2 \bmod m_2$
$x \equiv c_3 \bmod m_3$
.
.
$x \equiv c_n \bmod m_n$

The Chinese Remainder Theorem states:

If each pair of moduli m_i and m_j are relatively prime, $m_i \perp m_j$, then the equations have a solution and any two solutions are congruent mod $M = m_1 m_2 m_3 ... m_n$.

Proofs of the Chinese Remainder Theorem

In general theorems are not proven by examples. However, in the following two examples general method of solutions are used. Abstracting the methods into general proofs is a good exercise for the serious student.

Example Suppose we want to solve simultaneously the following three congruences:

$x \equiv 2 \bmod 5$

$x \equiv 4 \bmod 7$

$x \equiv 1 \bmod 9$

2 is a solution for the first congruence. From that we have that our general solution should be of the form x = 5y + 2. Substituting that into the second congruence we get $5y + 2 \equiv 4 \bmod 7$. This leads to $5y \equiv 2 \bmod 7$. The previous section tells us how to solve this type of problem using the extended Euclidean algorithm. However, usually we can find a solution directly. We keep adding 7 to the right-hand side until we get $5y \equiv 30 \bmod 7$. We can do this, because 7 mod 7 is the same as zero. We have y = 6 is a solution which implies y = 6 + 7z. Putting this in x = 5y + 2, we get x = 32 + 35z. Inserting this into the third congruence we get $32 + 35z \equiv 1 \bmod 9$. This leads to $5 + 8z \equiv 1 \bmod 9$. Hence $8z \equiv 5 \bmod 9$. We keep adding 9 to the right-hand side to until we get get $8z \equiv 32 \bmod 9$. This gives us $z \equiv 4 \bmod 9$, or z = 4 + 9w. Plugging this into x = 32 + 35z we get x = 172 + 315w. Note that 315 is the product of the three moduli, and our answer is then x = 172 mod 315. Note, that at each stage of this example we have a congruence of the form $cu \equiv v \bmod n$ where n is a product of terms relatively prime to c. However, the above theorem tells us that c must then be relatively prime to n. From this and the previous section we know that c must have an inverse mod n. It follows that there must be a solution to the problem.

Example Suppose we want to solve simultaneously the following three congruences:

$x \equiv 2 \bmod 4$

$x \equiv 3 \bmod 5$

$x \equiv 4 \bmod 7$

We will look for a solution of the form $C_1 \cdot 5 \cdot 7 + C_2 \cdot 4 \cdot 7 + C_3 \cdot 4 \cdot 5$. If we plug this into each of the expressions then two terms are congruent to zero. To make the expression solve our problem we need to solve for each of the parameters C_1, C_2, and

C_3, so that $C_1 \cdot 5 \cdot 7 \equiv 2 \bmod 4$, $C_2 \cdot 4 \cdot 7 \equiv 3 \bmod 5$ and $C_3 \cdot 4 \cdot 5 \equiv 4 \bmod 7$. Solving these using the same technique as in the last example we get, $C_1 = 2$, $C_2 = 1$, and $C_3 = 3$. Plugging these values into $C_1 \cdot 5 \cdot 7 + C_2 \cdot 4 \cdot 7 + C_3 \cdot 4 \cdot 5$, we get x = 158. This indeed satisfies the three congruences. However, so does the product of the moduli $4 \cdot 5 \cdot 7 = 140$. (Also, it is easy to show that this is the smallest number with that property.) Subtracting 140 from 158, we get 18, which is our smallest positive solution. Note that in using this technique we have to solve equations of the form $Ci \cdot a_1 \cdot a_2 \cdot \ldots \cdot a_k \equiv b \bmod a_n$. However, each of the terms a_j on the left is relatively prime to a_n. By the theorem proven at the beginning of the section a_n must be relatively prime to the product $a_1 \cdot a_2 \cdot \ldots \cdot a_k$. Hence the problem has a solution.

So what do we do for the problem of a deck with 40 cards as at the beginning of this chapter (since the Chinese Remainder Theorem does not apply)? Again we choose a number, x, from 0 to 39 (1 to 40 does not work in this scheme). By x div 4, we mean integer division by 4 (it can also be denoted x \ 4). For example, 7 div 2 = 3. If x is 25, we choose the suit by 25 mod 4 = 1 and the value by 25 div 4 = 6. The number 25 then corresponds to the 7 of diamonds.

The next three exercises are to solve systems of three equations.

☐ **Exercise 1**

$$x \equiv 1 \bmod 3$$
$$x \equiv 0 \bmod 4$$
$$x \equiv 2 \bmod 5$$

☐ **Exercise 2**

$$x \equiv 2 \bmod 5$$
$$x \equiv 3 \bmod 6$$
$$x \equiv 2 \bmod 7$$

☐ **Exercise 3**

$$x \equiv 3 \bmod 4$$
$$x \equiv 5 \bmod 9$$
$$x \equiv 9 \bmod 10$$

Appendix to Section 10

An Existence Proof of the Chinese Remainder Theorem

The following is just a restatement of the Chinese Remainder Theorem followed by an abstract proof.

Theorem: Suppose we are given k congruences: $x \equiv a_i \pmod{m_i}$ with i = 1,2,3...k. Suppose that we have that $m_i \perp m_j$ whenever $i \neq j$; then there is a solution Y which is unique (mod M) where $M = m_1 m_2 m_3 ... m_k$.

Proof: First we show that if there is a solution then it is unique (mod M). Suppose U and V are both solutions. Then $U \equiv V \pmod{m_i}$ for all i. But since the m_i are all pairwise relatively prime, $U \equiv V \pmod{M}$. Now consider the m_i as all fixed constants. The congruence involving m_j, $x \equiv a_j \pmod{m_j}$ can have m_j distinct values for a_j, that is to say a_j can take on the values 0, 1, 2, ..., m_j-1. Altogether then there are $m_1 m_2 m_3 ... m_k = M$ problems involving these moduli. However each number in the class 0 through M-1 is a solution to one of the M problems. Specifically, any integer X is a solution to the k congruences $X \equiv (X \bmod m_i) \pmod{m_i}$ with i = 1,2,3...k. In this expression X mod m_i is the function where *a mod b* means the remainder of a on division by b. Hence we have M distinct problems with the above set of moduli. We also have that each integer in the class 0,1,2,...M-1 is solution to such a problem. But since these solutions are unique (mod M) each problem has a unique solution in that class.

1. $x = 1 + 3y$. $3y \equiv 3 \bmod 4$. $y \equiv 1 \bmod 4$. $y = 1 + 4z$. $x = 4 + 12z$. $4 + 12z \equiv 2 \bmod 5$. $z \equiv 4 \bmod 5$. $z = 4 + 5u$. $x = 52 + 60u$. The answer is 52.

2. $x = 2 + 5y$. $2 + 5y \equiv 3 \bmod 6$. $5y \equiv 1 \bmod 6$. $y \equiv 5 \bmod 6$. $y = 5 + 6z$. $x = 27 + 30z$. $27 + 30z \equiv 2 \bmod 7$. $2z \equiv 3 \bmod 7$. $z \equiv 5 \bmod 7$. $z = 5 + 7u$. $x = 177 + 210u$. The answer is 177.

3. $x = 3 + 4y$. $3 + 4y \equiv 5 \bmod 9$. $4y \equiv 2 \bmod 9$. $y \equiv 5 \bmod 9$. $y = 5 + 9z$. $x = 3 + 4y = 23 + 36z$. $23 + 36z \equiv 9 \bmod 10$. $6z \equiv 6 \bmod 10$. $z \equiv 1 \bmod 10$. $z = 1 + 9u$. $x = 59 + 360u$. The answer is 59.