Chapter 18 Games

18.1 Flipping Coins over the Telephone

Alice is living in Anchorage and Bob is living in Baltimore. A friend, not realizing that they are no longer together, leaves them a car in his will. How do they decide who gets the car? Bob phones Alice and says he'll flip a coin. Alice chooses "Tails" but Bob says "Sorry, it was Heads." So Bob gets the car.

For some reason, Alice suspects Bob might not have been honest. (Actually, he told the truth; as soon as she called tails, he pulled out his specially made two-headed penny so he wouldn't have to lie.) She resolves that the next time this happens, she'll use a different method. So she goes to her local cryptologist, who suggests the following method.

Alice chooses two large random primes p and q, both congruent to 3 mod 4. She keeps them secret but sends the product $n = pq$ to Bob. Then Bob chooses a random integer x and computes $y \equiv x^2 \pmod{n}$. He keeps x secret but sends y to Alice. Alice knows that y has a square root mod n (if it doesn't, her calculations will reveal this fact, in which case she accuses Bob of cheating), so she uses her knowledge of p and q to find the four square roots $\pm a, \ \pm b$ of $y \pmod{n}$ (see Section 3.9). One of these will be x, but she doesn't know which one. She chooses one at random (this is the "flip"), say b, and sends it to Bob. If $b \equiv \pm x \pmod{n}$, Bob tells Alice that she wins. If $b \not\equiv \pm x \pmod{n}$, Bob wins.

$$\begin{array}{ccc}
\textbf{Alice} & & \textbf{Bob} \\
n = pq & \rightarrow & n \\
y & \leftarrow & y \equiv x^2 \\
a^2 \equiv b^2 \equiv y & \rightarrow & b \\
 & & \\
\text{Alice wins} & \leftarrow & b \equiv \pm x \\
\text{or} & & \text{or} \\
\text{Bob wins} & \leftarrow & b \not\equiv \pm x
\end{array}$$

But, asks Alice, how can I be sure Bob doesn't cheat? If Alice sends b to Bob and $x \equiv \pm a \pmod{n}$, then Bob knows all four square roots of $y \pmod{n}$, so he can factor n. In particular, $\gcd\,(x - b,\ n)$ gives a nontrivial factor of n. Therefore, if it is computationally infeasible to factor n, the only way Bob could produce the factors p and q would be when his value of x is not plus or minus the value of b that Alice sends. If Alice sends Bob $\pm x$, Bob has no more information than he had when Alice sent him the number n. Therefore, he should not be able to produce p and q in this case. So Alice can check that Bob didn't cheat by asking Bob for the factorization of n.

What if Alice tries to cheat by sending Bob a random number rather than a square root of y? This would surely prevent Bob from factoring n. Bob can guard against this by checking that the square of the number Alice sends is congruent to y.

Suppose Alice tries to deceive Bob by sending a product of three primes. Of course, Bob could ask Alice for the factorization of n at the end of the game; if Alice produces two factors, they can be quickly checked for primality. But Bob shouldn't worry about this possibility. When n is the product of three distinct primes, there are eight square roots of y. Therefore, up to sign there are four choices of numbers for Alice to send. Each of the three wrong choices will allow Bob to find a nontrivial factor of n. So Alice would decrease her chances of winning to only one in four. Therefore, she should not try this.

There is one flaw in this procedure. Suppose Bob decides he wants to lose. He can then claim his value of x was exactly the value that Alice sent him. Alice cannot dispute this since the only information she has is the square of Bob's number, which is congruent to the square of her number. There are other procedures that can prevent Bob from trying to lose, but we will not discuss them here.

Finally, we should mention that it is not difficult to find primes p and q that are congruent to 3 mod 4. The density of primes congruent to 1 mod 4 is the same as the density of primes that are 3 mod 4. Therefore, find a random prime p. If it is not 3 mod 4, try another. This process should succeed quickly. We can find q similarly.

Example

Alice chooses

$$p = 2038074743 \text{ and } q = 1190494759.$$

She sends

$$n = pq = 2426317299991771937$$

to Bob. Bob takes

$$x = 1414213562373095048$$

(this isn't as random as it looks; but Bob thinks the decimal expansions of square roots look random) and computes

$$y \equiv x^2 \equiv 363278601055491705 \pmod{n},$$

which he sends to Alice.

Alice computes

$$y^{(p+1)/4} \equiv 1701899961 (\bmod p) \text{ and } y^{(q+1)/4} \equiv 325656728 (\bmod q).$$

Therefore, she knows that

$$x \equiv \pm 1701899961 \pmod{p} \text{ and } x \equiv \pm 325656728 \pmod{q}.$$

The Chinese remainder theorem puts these together in four ways to yield

$$x \equiv \pm 1012103737618676889 \text{ or } \pm 937850352623334103 \pmod{n}.$$

Suppose Alice sends 1012103737618676889 to Bob. This is $-x \pmod{n}$, so Bob declares Alice the winner.

Suppose instead that Alice sends 937850352623334103 to Bob. Then Bob claims victory. By computing

$$\gcd(1414213562373095048 \; - \; 937850352623334103, n) = 1190494759,$$

he can prove that he won.

18.2 Poker over the Telephone

Alice and Bob quickly tire of flipping coins over the telephone and decide to try poker. Bob pulls out his deck of cards, shuffles, and deals two hands, one for Alice and one for himself. Now what does he do? Alice won't let him read the cards to her. Also, she suggests that he might not be playing with a full deck. Arguments ensue. But then someone suggests that they each choose their own cards. The betting is fast and furious. After several hundred coins (they remain unused from the coin-flipping protocol) have been wagered, Alice and Bob discover that they each have a royal flush. Each claims the other must have cheated. Fortunately, their favorite cryptologist can help.

Here is the method she suggests, in nonmathematical terms. Bob takes 52 identical boxes, puts a card in each box, and puts a lock on each one. He dumps the boxes in a bag and sends them to Alice. She chooses five boxes, puts her locks on them, and sends them back to Bob. He takes his locks off and sends the five boxes back to Alice, who takes her locks off and finds her five cards. Then she chooses five more boxes and sends them back to Bob. He takes off his locks and gets his five cards. Now suppose Alice wants to replace three cards. She puts three cards in a discard box, puts on her lock, and sends the box to Bob. She then chooses three boxes from the remaining 42 card boxes, puts on her locks, and sends them to Bob. Bob removes his locks and sends them back to Alice, who removes her locks and gets the cards. If Bob wants to replace two cards, he puts them in another discard box, puts on his lock, and sends the box to Alice. She chooses two card boxes and sends them to Bob. He removes his locks and gets his cards. They then compare hands to see who wins. We'll assume Alice wins.

After the hand has been played, Bob wants to check that Alice put three cards in her discard box since he wants to be sure she wasn't playing with eight cards. He puts his lock on the box and sends the box to Alice, who takes her lock off. Since Bob's lock is still on the box, she can't change the contents. She sends the box back to Bob, who removes the lock and finds the three cards that Alice discarded (this differs from standard poker in that Bob sees the actual cards discarded; in a standard game, Bob only sees that Alice discards three cards and doesn't need to look at them afterward). Similarly, Alice can check that Bob discarded two cards.

Bob can check that Alice played with the hand that was dealt by asking her to send her cards to him. Alice cannot change her hand since all the remaining cards still have Bob's locks on them (and Bob can't open them since Alice has them in her possession).

Of course, various problems arise if Alice or Bob unjustly accuses the other of cheating. But, ignoring such complications, we see that Alice and Bob can now play poker. However, the postage for sending 52 boxes back and forth is starting to cut into Alice's profits. So she goes back to her cryptologist and asks for a mathematical implementation. The following is the method.

Alice and Bob agree on a large prime p. Alice chooses a secret integer α with $\gcd(\alpha,\ p-1)=1$, and Bob chooses a secret integer β with $\gcd(\beta,\ p-1)=1$. Alice computes α' such that $\alpha\alpha' \equiv 1 \pmod{p-1}$ and Bob computes β' with $\beta\beta' \equiv 1 \pmod{p-1}$. A different α and β are used for each hand. A different p could be used for each hand also.

Note that $c^{\alpha\alpha'} \equiv c \pmod{p}$, and similarly for β. This can be seen as follows: $\alpha\alpha' \equiv 1 \pmod{p-1}$, so $\alpha\alpha' = 1+(p-1)k$ for some integer k. Therefore, when $c \not\equiv 0 \pmod{p}$

$$c^{\alpha\alpha'} \equiv c \cdot \left(c^{p-1}\right)^k \equiv c \cdot 1^k \equiv c \pmod{p}.$$

Trivially, we also have $c^{\alpha\alpha'} \equiv c \pmod{p}$ when $c \equiv 0 \pmod{p}$.

The 52 cards are changed to 52 distinct numbers $c_1, \ldots, c_{52} \mod p$ via some prearranged scheme. Bob computes $b_i \equiv c_i^\beta \pmod{p}$ for $1 \le i \le 52$, randomly permutes these numbers, and sends them to Alice. Alice chooses five numbers $b_{i_1}, \ldots, b_{i_5}$, computes $b_{i_j}^\alpha \pmod{p}$ for $1 \le j \le 5$, and sends these numbers to Bob. Bob takes off his lock by raising these numbers to the β' power and sends them to Alice, who removes her lock by raising to the α' power. This gives Alice her hand.

Alice then chooses five more of the numbers b_i and sends them back to Bob, who removes his locks by raising the numbers to the β' power. This gives him his hand. The rest of the game proceeds in this fashion.

It seems to be quite difficult for Alice to deduce Bob's cards. She could guess which encrypted card b_i corresponds to a fixed unencrypted card c_j. This means Alice would need to solve equations of the form $c_j^\beta \equiv b_i \pmod{p}$ for β. Doing this for the 52 choices for b_i would give at most 52 choices for β. The correct exponent β could then be determined by choosing another card $c_{j'}$ and trying the various possibilities for β to see which ones give the encrypted values that are on the list of encrypted cards. But these equations that Alice needs to solve are discrete logarithm problems, which are generally assumed to be difficult when p is large (see Chapter 10).

Example

Let's consider a simplified game where there are only five cards: ten, jack, queen, king, ace. Each player is dealt one card. The winner is the one with the higher card. Change the cards to numbers using $a = 01$, $b = 02$, $\ldots$, so we have the following:

Ten	Jack	Queen	King	Ace
200514	10010311	1721050514	11091407	10305

Let the prime be $p = 2396271991$. Alice chooses her secret $\alpha = 1234567$ and Bob chooses his secret $\beta = 7654321$. Alice computes $\alpha' = 402406273$ and Bob computes $\beta' = 200508901$. This can be done via the extended Euclidean algorithm. Just to be sure, Alice checks that $\alpha\alpha' \equiv 1 \pmod{p-1}$, and Bob does a similar calculation with β and β'.

Bob now calculates (congruences are mod p)

$$\begin{aligned} 200514^{\beta} &\equiv 914012224 \\ 10010311^{\beta} &\equiv 1507298770 \\ 1721050514^{\beta} &\equiv 74390103 \\ 11091407^{\beta} &\equiv 2337996540 \\ 10305^{\beta} &\equiv 1112225809. \end{aligned}$$

He shuffles these numbers and sends them to Alice:

$$1507298770, \quad 1112225809, \quad 2337996540, \quad 914012224, \quad 74390103.$$

Since Alice does not know β, it is unlikely she can deduce which card is which without a lot of computation.

Alice now chooses her card by choosing one of these numbers – for example, the fourth – raises it to the power α, and sends it to Bob:

$$914012224^{\alpha} \equiv 1230896099 \pmod{p}.$$

Bob takes off his lock by raising this to the power β' and sends it back to Alice:

$$1230896099^{\beta'} \equiv 1700536007 \pmod{p}.$$

Alice now removes her lock by raising this to the power α':

$$1700536007^{\alpha'} \equiv 200514 \pmod{p}.$$

Her card is therefore the ten.

Now Alice chooses Bob's card by simply choosing one of the original cards she received – for example, 1507298770 – and sending it back to Bob. Bob computes

$$1507298770^{\beta'} \equiv 10010311 \pmod{p}.$$

Therefore, his card is the jack.

This accomplishes the desired dealing of the cards. Alice and Bob now compare cards and Bob wins. To prevent cheating, Alice and Bob then reveal their secret exponents α and β. Suppose Alice tries to claim she has the king. Bob can quickly compute α' and show that the card he sent to Alice was the ten.

For another example of this game, see Example 39 in the Computer Appendices.

18.2.1 How to Cheat

No game of poker would be complete without at least the possibility of cheating. Here's how to do it in the present situation.

Bob goes to his local number theorist, who tells him about quadratic residues. A number $r \pmod{p}$ is called a **quadratic residue** mod p if the congruence $x^2 \equiv r \pmod{p}$ has a solution; in other words, r is a square mod p. A nonresidue n is an integer such that $x^2 \equiv n \pmod{p}$ has no solution.

There is an easy way to decide whether or not a number $z \not\equiv 0 \pmod{p}$ is a quadratic residue or nonresidue:

$$z^{(p-1)/2} \equiv \begin{cases} +1 \pmod{p} & \text{if } z \text{ is a quadratic residue} \\ -1 \pmod{p} & \text{if } z \text{ is a quadratic nonresidue} \end{cases}$$

(see Exercise 1). This determination can also be done using the Legendre or Jacobi symbol plus quadratic reciprocity. See Section 3.10.

Recall that we needed $\gcd(\alpha,\ p-1)=1$ and $\gcd(\beta,\ p-1)=1$. Therefore, α and β are odd. A card c is encrypted to c^{β}, and

$$\left(c^{\beta}\right)^{(p-1)/2} \equiv \left(c^{(p-1)/2}\right)^{\beta} \equiv c^{(p-1)/2} \pmod{p},$$

since $(\pm 1)^{\text{odd}} \equiv \pm 1$ (with the same choice of signs on both sides of the congruence). Therefore, c is a quadratic residue mod p if and only if c^{β} is a quadratic residue. The corresponding statement also applies to the α and $\alpha\beta$ power of the cards.

When Alice sends Bob the five cards that will make up her hand, Bob quickly checks these cards to see which are quadratic residues and which are nonresidues. This means that there are two sets R and N, and for each of Alice's cards, he knows whether the card is in R or N. This gives him a slight advantage. For example, suppose he needs to know whether or not she has the queen of hearts and he determines that it is in N. If she has only one N card, the chances are low that she has the card. In this way, Bob obtains a slight advantage and starts winning.

Alice quickly consults her local cryptologist, who fortunately knows about quadratic residues, too. Now when Alice chooses Bob's hand, she arranges that all of his cards are in R, for example. Then she knows that his hand is chosen from 26 cards rather than 52. This is better than the partial information that Bob has and is useful enough that she gains an advantage over Bob. Finally, Alice gets very bold. She sneakily chooses the prime p so that the ace, king, queen, jack, and ten of spades are the only quadratic residues. When she chooses Bob's hand, she gives him five nonresidues. She chooses the five residues for herself. Bob, who has been computing residues and nonresidues on each hand, has already been getting suspicious since his cards have all been residues or all been nonresidues for several hands. But now he sees before the hand is played that she has chosen a royal flush for herself. He accuses her of cheating, arguments ensue, and they go back to coin flipping.

Example

Let's return to the simplified example. The choice of prime p was not random. In fact,

$$\begin{aligned} 200514^{(p-1)/2} &\equiv 1 \\ 10010311^{(p-1)/2} &\equiv 1 \\ 1721050514^{(p-1)/2} &\equiv 1 \\ 11091407^{(p-1)/2} &\equiv 1 \\ 10305^{(p-1)/2} &\equiv -1, \end{aligned}$$

so only the ace is a nonresidue, while all the remaining cards are quadratic residues.

When Alice is choosing her hand, she computes

$$\begin{aligned} 1507298770^{(p-1)/2} &\equiv 1 \\ 1112225809^{(p-1)/2} &\equiv -1 \\ 2337996540^{(p-1)/2} &\equiv 1 \\ 914012224^{(p-1)/2} &\equiv 1 \\ 74390103^{(p-1)/2} &\equiv 1. \end{aligned}$$

This tells her that the ace is 1112225809. She raises it to the power α', then sends it to Bob. He raises it to the power β' and sends it back to Alice, who raises it to the power α'. Of course, she finds that her card is the ace.

For more on playing poker over the telephone, see [Fortune-Merritt].

18.3 Exercises

1. Let α be a primitive root for the prime p. This means that the numbers $1, \alpha, \alpha^2, \alpha^3, \ \ldots\ , \alpha^{p-2} \pmod p$ yield all of the nonzero congruence classes mod p.

    1. Let i be fixed and suppose $x^2 \equiv \alpha^i \pmod p$ has a solution x. Show that i must be even. (Hint: Write $x \equiv \alpha^j$ for some j. Now use the fact that $\alpha^k \equiv \alpha^l \pmod p$ if and only if $k \equiv l \pmod{p-1}$.) This shows that the nonzero squares mod p are exactly $1, \alpha^2, \alpha^4, \alpha^6, \ \ldots\ \pmod p$, and therefore $\alpha, \alpha^3, \alpha^5, \ \ldots$ are the quadratic nonresidues mod p.

    2. Using the definition of primitive root, show that $\alpha^{(p-1)/2} \not\equiv 1 \pmod p$.

    3. Use Exercise 15 in Chapter 3 to show that $\alpha^{(p-1)/2} \equiv -1 \pmod p$.

    4. Let $x \not\equiv 0 \pmod p$. Show that $x^{(p-1)/2} \equiv 1 \pmod p$ if x is a quadratic residue and $x^{(p-1)/2} \equiv -1 \pmod p$ if x is a quadratic nonresidue mod p.

2. In the coin flipping protocol with $n = pq$, suppose Bob sends a number y such that neither y nor $-y$ has a square root mod n.

    1. Show that y cannot be a square both mod p and mod q. Similarly, $-y$ cannot be a square mod both primes.

    2. Suppose y is not a square mod q. Show that $-y$ is a square mod q.

    3. Show that y is a square mod one of the primes and $-y$ is a square mod the other.

    4. Benevolent Alice decides to correct Bob's "mistake." Suppose y is a square mod p and $-y$ is a square mod q. Alice calculates a number b such that $b^2 \equiv y \pmod p$ and $b^2 \equiv -y \pmod q$ and sends b to Bob (there are two pairs of choices for b). Show how Bob can use this information to factor n and hence claim victory.

3.
    1. Let p be an odd prime. Show that if $x \equiv -x \pmod p$, then $x \equiv 0 \pmod p$.

2. Let p be an odd prime. Suppose $x, y \not\equiv 0 \pmod{p}$ and $x^2 \equiv y^2 \pmod{p^2}$. Show that $x \equiv \pm y \pmod{p^2}$ (Hint: Look at the proof of the Basic Principle in Section 9.3.)

3. Suppose Alice cheats when flipping coins by choosing $p = q$. Show that Bob always loses in the sense that Alice always returns $\pm x$. Therefore, it is wise for Bob to ask for the two primes at the end of the game.