MATH 406: Coin Flipping

1. **Theorem:**

   Suppose p and q are distinct primes congruent to 3 mod 4 and $n = pq$. Let A satisfy $\gcd(A, n) = 1$ (hence also $p \nmid A$ and $q \nmid A$). Suppose $x^2 \equiv A \bmod n$ has solutions. Then it has exactly four incongruent solutions.

   Proof:

   First note that we have:

   $$\forall x, \left[x^2 \equiv A \bmod n \quad \Longleftrightarrow \quad \left[x^2 \equiv A \bmod p \text{ and } x^2 \equiv A \bmod q\right]\right]$$

   This follows immediately since $n = pq$ with p, q distinct primes.

   Assuming then that the equation on the left has at least one solution we know that the pair on the right has at least one solution.

   To say $x^2 \equiv A \bmod p$ has a solution means that A is a quadratic residue mod p and will have exactly two incongruent solutions mod p. Likewise for the second, mod q.

   In fact we can solve these two equations easily. For the first, observe that, using Euler's Criterion:

   $$\left(\pm A^{(p+1)/4}\right)^2 \equiv A^{(p+1)/2} \equiv A \cdot A^{(p-1)/2} \equiv A \left(\frac{A}{p}\right) \equiv A \cdot 1 \equiv A \bmod p$$

   Moreover if $+A^{(p+1)/4} \equiv -A^{(p+1)/4} \bmod p$ then $p \mid 2A^{(p+1)/4}$ which contradicts the fact that $p \nmid 2$ and $p \nmid A$ so these are incongruent mod p. Thus $x^2 \equiv A \bmod p$ has the two incongruent solutions $x \equiv \pm A^{(p+1)/4} \bmod p$ and similarly $x^2 \equiv A \bmod q$ has the two incongruent solutions $x \equiv \pm A^{(q+1)/4} \bmod q$.

   Paring them up, consider the following four systems:

$x \equiv +A^{(p+1)/4} \bmod p$ $x \equiv +A^{(q+1)/4} \bmod q$	$x \equiv +A^{(p+1)/4} \bmod p$ $x \equiv -A^{(q+1)/4} \bmod q$	$x \equiv -A^{(p+1)/4} \bmod p$ $x \equiv -A^{(q+1)/4} \bmod q$	$x \equiv -A^{(p+1)/4} \bmod p$ $x \equiv +A^{(q+1)/4} \bmod q$

   Each can be solved using the Chinese Remainder Theorem and each yields a unique solution mod $n = pq$. These four solutions differ because they satisfy different systems. Moreover each will then solve the system:

   $$x^2 \equiv A \bmod p$$
   $$x^2 \equiv A \bmod q$$

   And since $\gcd(p, q) = 1$ each also satisfies the original target equation $x^2 \equiv A \bmod n = pq$.

   Moreover since the third system is the negation of the first and since the fourth system is the negation of the second, the solution to the third system will be the negation of the solution to the second and the solution to the fourth systems will be the negation of the solution to the second

   Thus we simply solve the first two, call their solutions $+X$ and $+Y$, and then use $-X$ and $-Y$ for the other two.

   QED

Example:

Suppose $p = 31$ and $q = 43$. Let $n = pq = 1333$. It is a fact that $x^2 \equiv 669 \bmod 1333$ has solutions. Let's find all four.

- We solve the first system:

$$\begin{aligned} x &\equiv +669^{(31+1)/4} \equiv 7 \bmod 31 \\ x &\equiv +669^{(43+1)/4} \equiv 14 \bmod 43 \end{aligned}$$

  The CRT gives us $x \equiv 100 \bmod 1333$.

- We solve the second system:

$$\begin{aligned} x &\equiv +669^{(31+1)/4} \equiv 7 \bmod 31 \\ x &\equiv -669^{(43+1)/4} \equiv -14 \bmod 43 \end{aligned}$$

  The CRT gives us $x \equiv 1061 \bmod 1333$.

Thus our four solutions are:

$$\begin{aligned} +X &\equiv 100 \bmod 1333 \\ -X &\equiv -100 \equiv 1233 \bmod 1333 \\ +Y &\equiv 1061 \bmod 1333 \\ -Y &\equiv -1061 \equiv 272 \bmod 1333 \end{aligned}$$

2. **Theorem:**

Suppose p and q are distinct primes congruent to 3 mod 4 and $n = pq$. Let A satisfy $\gcd(A, n) = 1$. Consider the equation $x^2 \equiv A \bmod n$ with four incongruent solutions $\{+X, -X, +Y, -Y\}$.

Then factoring n is equivalent to finding one of $\pm X$ and one of $\pm Y$).

Proof:

$\Longrightarrow$

Suppose we can factor n. Then we just solve the system using the process developed and hence we actually find all of $\{+X, -X, +Y, -Y\}$.

$\Longleftarrow$

Suppose we know one of $\pm X$ and one of $\pm Y$. Then we can factor n.

Let's examine the case where we know $+X$ and $+Y$. First, observe that $+X + (+Y) \equiv 2A^{(p+1)/4} \not\equiv 0 \bmod p$ because $p \nmid 2A^{(p+1)/4}$ as noted earlier. Thus $p \nmid (+X + (+Y))$. Second, observe that $+X + (+Y) \equiv 0 \bmod q$ and so $q \mid (+X + (+Y))$. Thus $\gcd(+X + (+Y), n) = q$ which can be found by the Euclidean Algorithm.

A similar argument works for $+X, -Y$, $-X, +Y$ and $-X, -Y$. With details omitted.

In other words $\gcd(+X + (+Y), n)$, $\gcd(+X + (-Y), n)$, $\gcd(-X + (-Y), n)$, and $\gcd(-X + (+Y), n)$ will yield either p or q.

$\mathcal{QED}$

3. **Theorem Follow-Up:**

   If we are given two of $\{+X, -X, +Y, -Y\}$, possibly with repeats, there is a 50% chance that we will get one of $\pm X$ and one of $\pm Y$ and then the gcd calculations above will give us p or q.

   On the other hand if we given some other two then taking gcds of sums and differences with n will not give us p or q but rather will give us 1 or n, which will not help us factor n. This argument is similar to the above: For example if we know $+X$ and $-X$ then $+X + (-X) \equiv 0 \bmod p$ and $+X + (-X) \equiv 0 \bmod q$ so $\gcd(+X + (-X), n) = n$ and $+X - (-X) \equiv 2A^{(p+1)/4} \not\equiv 0 \bmod p$ and $+X - (-X) \equiv 2A^{(p+1)/4} \not\equiv 0 \bmod q$ so $\gcd(+X - (-X), n) = 1$.

   In practice therefore if we are given $\alpha, \beta \in \{+X, -X, +Y, -Y\}$ then by testing $\gcd(\alpha \pm \beta, n)$ there is a 50% chance that we will get either p or q.

   Note that we don't need to check $\gcd(-\alpha \pm \beta, n)$ because $\gcd(-\alpha \pm \beta, n) = \gcd(\alpha \mp \beta, n)$.

4. **Coin Flip Process:**

   We then proceed as follows:

   (a) Alice picks two large primes p and q both congruent to 3 mod 4 and calculates $n = pq$. She sends n to Bob.

   (b) Bob picks some α with $\gcd(\alpha, n) = 1$ and sends the least nonnegative residue $A \equiv \alpha^2 \bmod n$ back to Alice.

   (c) Alice solves the equation $x^2 \equiv A \bmod n$ which she can do because she knows p, q.

   (d) At this point note that Bob knows just one solution $\alpha \in \{+X, -X, +Y, -Y\}$ whereas Alice knows all four. However she does not know which one Bob knows.

   (e) Alice picks one, call it β. She has an equal chance of choosing one that will help Bob factor n and one that will not. She sends that one back to Bob.

   (f) If Bob can factor n with what he has by testing gcds then he wins the coin flip. Otherwise Alice wins. Really he just tests $\gcd(\alpha \pm \beta, n)$ and sees if he gets something other than 1 or n.

5. **Example:**

   Alice chooses $p = 31$ and $q = 43$ and calculate $n = pq = 1333$. She sends this to Bob. Bob picks $\alpha = 100$ and calculates $\alpha^2 \equiv 669 \bmod 1333$ and sends 669 back to Alice. Alice solves $x^2 \equiv 669 \bmod 1333$ and gets solutions $100, 272, 1061, 1233$. She knows one of these is Bob's α but doesn't know which. She chooses one of them and sends it back. If she sends back 100 or 1233 then Bob cannot factor n. However if she sends back 272 or 1061 then he can. Observe:

   - If she sends $\beta = 100$ then Bob has nothing new. He loses.
   - If she sends $\beta = 1233$ then Bob tests $\gcd(100 \pm 1233, 1333)$ and these equal 1 or 1333. He loses.
   - If she sends $\beta = 272$ then Bob tests $\gcd(100 \pm 272, 1333)$ and notes that the results are 31 or 43. He wins.
   - If she sends $\beta = 1061$ then Bob tests $\gcd(100 \pm 1061, 1333)$ and notes that the results are 31 or 43. He wins.