FINDING ALL SQUARE ROOTS (mod \( pq \)) IS AS HARD AS FACTORING

Question: Let \( p, q \) be primes and let \( 1 \leq a < pq \) with \( \text{GCD}(a, pq) = 1 \). How many solutions \( 1 \leq x \leq pq \) are there to the equation

\[ x^2 \equiv a \pmod{pq} \]

Let’s do some examples to see if we can formulate a conjecture about this.

Example 1: Let \( 1 \leq x < 15 \). Solve \( x^2 \equiv 1 \pmod{15} \). With a brute force search, we find the four solutions \( x = 1, 4, 11, 14 \). These can be written \( x \equiv \pm 1, \pm 4 \pmod{15} \).

Example 2: Let \( 1 \leq x < 15 \). Solve \( x^2 \equiv 2 \pmod{15} \). A brute force search shows there are no solutions.

Example 3: Let \( 1 \leq x < 15 \). Solve \( x^2 \equiv 4 \pmod{15} \). With a brute search, we find the four solutions \( x = 2, 7, 8, 13 \). These can be written \( x \equiv \pm 2, \pm 7 \pmod{15} \).

Example 4: Let \( 1 \leq x < 15 \). Solve \( x^2 \equiv 7 \pmod{15} \) and \( x^2 \equiv 8 \pmod{15} \) and \( x^2 \equiv 11 \pmod{15} \) and \( x^2 \equiv 13 \pmod{15} \) and \( x^2 \equiv 14 \pmod{15} \) A brute force search shows there are no solutions for all these cases.

Conjecture: Let \( p, q \) be primes. Let \( 1 \leq a < pq \) with \( \gcd(a, pq) = 1 \). Then the equation \( x^2 \equiv a \pmod{pq} \) either has exactly 4 solutions or no solutions with \( 1 \leq x < pq \).

Remark: The above conjecture can be proved (see section 3.9 in the Trappe-Washington book).

We now prove that finding 4 square roots (mod \( pq \)) (if they exist) is as hard as factoring \( pq \).

Proof: Let \( \pm u, \pm v \) be the four square roots of \( a \pmod{pq} \), i.e.,

\[ u^2 \equiv a \pmod{pq}, \quad v^2 \equiv a \pmod{pq} \quad \Rightarrow \quad u^2 - v^2 \equiv 0 \pmod{pq}. \]

For the four square roots to be distinct (mod \( pq \)) it is necessary that \( u \neq \pm v \pmod{pq} \).

Now \( u^2 - v^2 \equiv 0 \pmod{pq} \) implies that

\[ (u - v)(u + v) \equiv 0 \pmod{pq}. \]

This means that \( u - v \) must be divisible by either \( p \) or \( q \) but not both. So we can factor \( pq \) by computing \( \gcd(u - v, pq) \).

Example: Factor \( n = 77 \) by finding the four solutions to \( x^2 \equiv 1 \pmod{77} \). Clearly \( x \equiv \pm 1 \pmod{77} \) are two solutions, i.e., \( x = 1, 76 \). With a brute force search we find the other two solutions \( x \equiv \pm 34 \pmod{77} \), i.e., \( x = 34, 43 \). Then

\[ 34^2 - 1^2 \equiv 0 \pmod{77}. \]

When we compute

\[ \gcd(34 - 1, n) = 11 \]

we find the factorization of \( n = 77 \).