Taking square roots of -1

THINH D. NGUYEN*

Moscow State University
kosmofarmer@gmail.com

July 19, 2018

Abstract

Number-theoretic computational problems have the centralized position among various research areas of the theory of computing. Soviet-era mathematicians had contributed to that specific sub-field. After the dissolution of it, post-Soviet ones manage to push the field much further. In this article, we are humble to point out that if one has ever loved reading books of Prasolov, one would hesitate to count the number of solutions, even if one knows, a priori, that the exact result will be a power of 2.

I. PROPOSITIONS

Consider the ring $\mathbb{Z}/n$ of integers modulo some number n . Our question is whether there exists a square root of -1 in $\mathbb{Z}/n$. Equivalently, we want to ask whether there exists an integer x such that n divides $x^2 + 1$. For example, we have $2^2 \equiv -1 \pmod{5}$, but there is no number which squares to -1 modulo 7.

DEFINITION

Our problem will be denoted SQRT OF -1. It is the set of binary representations of natural numbers n such that -1 is a square modulo n .

We will consider cases of n according to its prime factorization.

POWERS of 2

First, observe that in the case $n = 2$ we actually have $1 \equiv -1$ so that a square root of -1 trivially exists. Next, consider the case $n = 2^\alpha$. Note that $x^2 + 1$ modulo 4 is either 1 or 2 depending on whether x is even or odd. In any case, $x^2 + 1$ is not

*Perebor

divisible by 4 which shows that there are no square roots of -1 in the case $n = 2^\alpha$ when $\alpha > 1$.

PRIME NUMBERS

The following is a standard theorem that answers our question for n an odd prime. This can be seen as the crucial case.

Theorem: Let p be a prime. The equation $x^2 \equiv -1$ has a solution in $\mathbb{Z}/p$ iff. $p \equiv 1 \pmod{4}$, in which case there are exactly two solutions.

Proof: First, we are going to show that -1 is the unique element of order 2 in $(\mathbb{Z}/p)^\times$. Let x be such an element of order 2. Then p divides $x^2 - 1$ and hence p divides either $x - 1$ or $x + 1$ which implies that $x = 1$ or $x = -1$. Being of order 2, $x = -1$. Alternately, one could just note that $x^2 - 1$ can have at most two roots in the field $\mathbb{Z}/p$.

Therefore, an element x of $\mathbb{Z}/p$ satisfies $x^2 \equiv -1$ iff. it is of order 4 in $(\mathbb{Z}/p)^\times$. Assume that we have such an element of order 4. This implies that 4 divides $|(\mathbb{Z}/p)^\times| = p - 1$. The claimed necessity of $p \equiv 1 \pmod{4}$ follows.

Now, suppose $p \equiv 1 \pmod{4}$. Consider the group

$$G = (\mathbb{Z}/p)^\times / \{-1, +1\}$$

Its order $|G| = (p - 1)/2$ is even which implies that G contains at least one element g of order 2. Let x be in the preimage of g under the quotient map. The order of x can only be 2 or 4. If it were 2 then $x = -1$ which would imply the contradiction that $g = 1$. Consequently, x is of order 4 and $\pm x$ (which are distinct) are our sought solutions. Since $\mathbb{Z}/p$ is a field there cannot be further solutions. **Q.E.D**

PRIME POWERS

Examining the previous proof, we can generalize to the case of prime powers $n = p^\alpha$.

Theorem: Let p be an odd prime. The equation $x^2 = -1$ has a solution in $\mathbb{Z}/p^\alpha$ iff. $p \equiv 1 \pmod{4}$, in which case there are exactly two solutions.

Proof: Again, we claim that -1 is the unique element of order 2 in $(\mathbb{Z}/p^\alpha)^\times$. If x is such an element then p^α divides $x^2 - 1$ and hence p^α divides either $x - 1$ or $x + 1$ (note that p cannot divide both $x - 1$ and $x + 1$). We conclude $x = -1$.

Therefore, an element x of $\mathbb{Z}/p^\alpha$ satisfies $x^2 \equiv -1$ iff. it is of order 4 in $(\mathbb{Z}/p^\alpha)^\times$. Assume that we have such an element of order 4. This implies that 4

divides $|(\mathbb{Z}/p^\alpha)^\times| = p^{\alpha-1}(p-1)$. The claimed necessity of $p \equiv 1 \pmod{4}$ again follows.

Now, suppose $p \equiv 1 \pmod{4}$. Consider the group

$$G = (\mathbb{Z}/p^\alpha)^\times / \{-1, +1\}$$

Its order $|G| = p^{\alpha-1}(p-1)/2$ is even which implies that G contains at least one element g of order 2. Let x be in the preimage of g under the quotient map. The order of x can only be 2 or 4. If it were 2 then $x = -1$ which would imply the contradiction that $g = 1$. Consequently, x is of order 4 and $\pm x$ (which are distinct) are two solutions. To see that there are no further elements of order 4, suppose x and y are of order 4. It follows from $x^2 = y^2 = -1$ that $(xy)^2 = 1$, and hence $xy = \pm 1$. This implies $y = \pm x$. **Q.E.D**

GENERAL CASE

We are now able to prove the following theorem.

Theorem: The equation $x^2 = -1$ has a solution in $\mathbb{Z}/n$ iff. n decomposes as

$$n = 2^\epsilon p_1^{\alpha_1} \dots p_s^{\alpha_s}$$

where $\epsilon \in \{0, 1\}$ and the p_j are primes satisfying $p_j \equiv 1 \pmod{4}$. In this case, there are exactly 2^s solutions where s is the number of distinct primes among the p_j 's.

Proof: This is an immediate consequence of our previous discussion, and the Chinese Remainder Theorem. If $n = n_1 n_2$ for relatively prime n_1 and n_2 , then n divides $x^2 + 1$ iff. both n_1 and n_2 divide $x^2 + 1$. We conclude that n is of the claimed form in order for a solution of $x^2 \equiv -1$ to exist.

On the other hand, given that $n = 2^\epsilon p_1^{\alpha_1} \dots p_s^{\alpha_s}$ for distinct primes p_j such that $p_j \equiv 1 \pmod{4}$, we find exactly two solutions for each of the s equations

$$x^2 \equiv -1 \pmod{p_j^{\alpha_j}}.$$

Using the isomorphism given by the Chinese Remainder Theorem, these combine to exactly 2^s solutions of $x^2 \equiv -1$ modulo n . **Q.E.D**

And now, to say something related to computing, we have shown that $\text{SQRT OF -1} \leq_p \text{FACTORING}$. Other corollaries about squarefreeness, number of distinct prime divisor, counting, etc. are left to the mathematics community.

II. CONCLUSION

As long as we do the research on a well-known conjecture, we should recall our mathematical nature from Kvant, Prasolov-style of doing mathematics, similar to mathematics of [2] back to those beautiful days.

REFERENCES

- [1] Michael R. Garey, David S. Johnson, **Computers and Intractability: A Guide to the Theory of NP-Completeness**
- [2] Phan Dinh Dieu, Le Cong Thanh, Le Tuan Hoa, **Average Polynomial Time Complexity of Some NP-Complete Problems**. Theor. Comput. Sci. 46(3): 219-237 (1986)