

Number theory and Cryptography

Chao Qin

School of Mathematical Sciences

May 30th, 2024



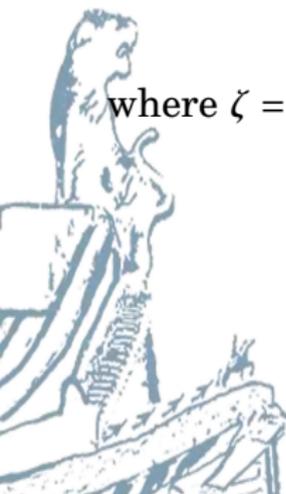
Finding Square Roots

Definition (Gauss Sum)

Fix an odd prime p . The *Gauss sum* associated to an integer a is

$$g_a = \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) \zeta^{an},$$

where $\zeta = \zeta_p = \cos(2\pi/p) + i \sin(2\pi/p) = e^{2\pi i/p}$.



Finding Square Roots

Definition (Gauss Sum)

Fix an odd prime p . The *Gauss sum* associated to an integer a is

$$g_a = \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) \zeta^{an},$$

where $\zeta = \zeta_p = \cos(2\pi/p) + i \sin(2\pi/p) = e^{2\pi i/p}$.

Proposition (Gauss Sum)

For any a not divisible by p ,

$$g_a^2 = (-1)^{(p-1)/2} p.$$

Finding Square Roots

Lemma

For any integer a ,

$$\sum_{n=0}^{p-1} \zeta^{an} = \begin{cases} p & \text{if } a \equiv 0 \pmod{p}, \\ 0 & \text{otherwise.} \end{cases}$$



Finding Square Roots

Proof.

If $a \equiv 0 \pmod{p}$, then $\zeta^a = 1$, so the sum equals the number of summands, which is p . If $a \not\equiv 0 \pmod{p}$, then we use the identity

$$x^p - 1 = (x - 1)(x^{p-1} + \dots + x + 1)$$

with $x = \zeta^a$. We have $\zeta^a \neq 1$, so $\zeta^a - 1 \neq 0$ and

$$\sum_{n=0}^{p-1} \zeta^{an} = \frac{\zeta^{ap} - 1}{\zeta^a - 1} = \frac{1 - 1}{\zeta^a - 1} = 0.$$

□

Finding Square Roots

Lemma

If x and y are arbitrary integers, then

$$\sum_{n=0}^{p-1} \zeta^{(x-y)n} = \begin{cases} p & \text{if } x \equiv y \pmod{p}, \\ 0 & \text{otherwise.} \end{cases}$$



Finding Square Roots

Lemma

If x and y are arbitrary integers, then

$$\sum_{n=0}^{p-1} \zeta^{(x-y)n} = \begin{cases} p & \text{if } x \equiv y \pmod{p}, \\ 0 & \text{otherwise.} \end{cases}$$

Proof.

This follows from last Lemma by setting $a = x - y$. □

Finding Square Roots

Lemma

If x and y are arbitrary integers, then

$$\sum_{n=0}^{p-1} \zeta^{(x-y)n} = \begin{cases} p & \text{if } x \equiv y \pmod{p}, \\ 0 & \text{otherwise.} \end{cases}$$

Proof.

This follows from last Lemma by setting $a = x - y$. □

Lemma

We have $g_0 = 0$.

Finding Square Roots

Proof.

By definition

$$g_0 = \sum_{n=0}^{p-1} \left(\frac{n}{p}\right). \quad (1)$$

the map

$$\left(\frac{\cdot}{p}\right) : (\mathbf{Z}/p\mathbf{Z})^* \rightarrow \{\pm 1\}$$

is a surjective homomorphism of groups. Thus, half the elements of $(\mathbf{Z}/p\mathbf{Z})^*$ map to $+1$ and half map to -1 (the subgroup that maps to $+1$ has index 2). Since $\left(\frac{0}{p}\right) = 0$, the sum is 0. \square

Finding Square Roots

Lemma

For any integer a ,

$$g_a = \left(\frac{a}{p}\right) g_1.$$



Finding Square Roots

Proof.

When $a \equiv 0 \pmod{p}$, the lemma follows from last Lemma, so suppose that $a \not\equiv 0 \pmod{p}$. Then,

$$\left(\frac{a}{p}\right) g_a = \left(\frac{a}{p}\right) \sum_{n=0}^{p-1} \left(\frac{n}{p}\right) \zeta^{an} = \sum_{n=0}^{p-1} \left(\frac{an}{p}\right) \zeta^{an} = \sum_{m=0}^{p-1} \left(\frac{m}{p}\right) \zeta^m = g_1.$$

Here, we use that multiplication by a is an automorphism of $\mathbf{Z}/p\mathbf{Z}$. Finally, multiply both sides by $\left(\frac{a}{p}\right)$ and use that

$$\left(\frac{a}{p}\right)^2 = 1.$$

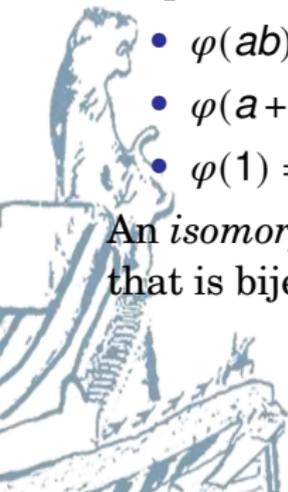
□

Definition (Homomorphism of Rings)

Let R and S be rings. A *homomorphism of rings* $\varphi : R \rightarrow S$ is a map such that for all $a, b \in R$, we have

- $\varphi(ab) = \varphi(a)\varphi(b)$,
- $\varphi(a + b) = \varphi(a) + \varphi(b)$, and
- $\varphi(1) = 1$.

An *isomorphism* $\varphi : R \rightarrow S$ of rings is a ring homomorphism that is bijective.



Finding Square Roots

Example

Continuing Example 1, we find a square root of 69 modulo 389. We apply the algorithm described above in the case $p \equiv 1 \pmod{4}$. We first choose the random $z = 24$ and find that $(1 + 24\alpha)^{194} = -1$. The coefficient of α in the power is 0, and we try again with $z = 51$. This time, we have $(1 + 51\alpha)^{194} = 239\alpha = u + v\alpha$. The inverse of 239 in $\mathbf{Z}/389\mathbf{Z}$ is 153, so we consider the following three possibilities for a square root of 69:

$$-\frac{u}{v} = 0 \quad \frac{1-u}{v} = 153 \quad \frac{-1-u}{v} = -153.$$

Thus, 153 and -153 are the square roots of 69 in $\mathbf{Z}/389\mathbf{Z}$.