Index Calculus and Power Residues

Ryan C. Daileda

Trinity University

Number Theory

The Exponential Map

Let $G = \langle a \rangle$ be a cyclic group of order m.

Since $a^j = a^k$ iff $j \equiv k \pmod{m}$, we find that the map

$$\begin{aligned} \exp_a : \mathbb{Z}/m\mathbb{Z} &\to G, \\ k + m\mathbb{Z} &\mapsto a^k, \end{aligned}$$

is a well-defined surjection.

Because $|\mathbb{Z}/m\mathbb{Z}| = m = |G|$, the pigeonhole principle implies that $\exp_a$ is actually a bijection.

Notice that

$$\begin{aligned} \exp_a((j + m\mathbb{Z}) + (k + m\mathbb{Z})) &= \exp_a((j + k) + m\mathbb{Z}) \\ &= a^{j+k} = a^j a^k = \exp_a(j + m\mathbb{Z}) \exp_a(k + m\mathbb{Z}). \end{aligned}$$

This proves the following result.

Theorem 1

Let $G = \langle a \rangle$ be a cyclic group of order m. The map

$$\exp_a : \mathbb{Z}/m\mathbb{Z} \to G$$

is an additive-to-multiplicative group isomorphism.

Remarks.

- When $G = \langle a \rangle$ is an *infinite* cyclic group, a similar argument shows that the map $\exp_a : \mathbb{Z} \to G$ given by $\exp_a(k) = a^k$ is also an isomorphism.
- Together these result say that, up to isomorphism, the *only* cyclic groups are $\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z}$ for $m \in \mathbb{N}$.

The Index

The inverse of the exponential map $\exp_a$ is the *discrete logarithm* or *index*.
It is given by

$$\begin{aligned} \mathrm{ind}_a : G &\to \mathbb{Z}/m\mathbb{Z}, \\ a^k &\mapsto k + m\mathbb{Z}. \end{aligned}$$

Because the inverse of an isomorphism is another isomorphism, we immediately have the following result.

Theorem 2 (Properties of the Index)

Suppose that $G = \langle a \rangle$ is a cyclic group. Then for all $x, y \in G$ one has:

1. $\mathrm{ind}_a(xy) = \mathrm{ind}_a(x) + \mathrm{ind}_a(y)$.
2. $\mathrm{ind}_a(x^k) = k\,\mathrm{ind}_a(x)$ *for all* $k \in \mathbb{Z}$.
3. $\mathrm{ind}_a(e) = 0$ *and* $\mathrm{ind}_a(a) = 1$.

Indices Relative to Primitive Roots

Let $n \in \mathbb{N}$. If n has a primitive root a, we can take

$$G = (\mathbb{Z}/n\mathbb{Z})^\times = \langle a + n\mathbb{Z} \rangle.$$

Since $m = |G| = \varphi(n)$, in this case the index provides an isomorphism

$$\mathrm{ind}_a : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{Z}/\varphi(n)\mathbb{Z}.$$

Remarks.

- When n is understood, we will usually write $\mathrm{ind}_a(x)$ for $\mathrm{ind}_a(x + n\mathbb{Z})$, and will frequently represent $\mathrm{ind}_a(x)$ by any one of its members.
- Be aware that the textbook defines $\mathrm{ind}_a(x)$ to be the *least nonnegative* member of $\mathrm{ind}_a(x + n\mathbb{Z})$.

Example

Since $(\mathbb{Z}/7\mathbb{Z})^\times = \langle 3 + 7\mathbb{Z}\rangle$ and

$$3^2 \equiv 2 \pmod 7,\ 3^3 \equiv 6 \pmod 7,$$
$$3^4 \equiv 4 \pmod 7,\ 3^5 \equiv 5 \pmod 7,$$

we find that

$$\mathrm{ind}_3(1) = 0,\ \ \mathrm{ind}_3(2) = 2,\ \ \mathrm{ind}_3(3) = 1,$$
$$\mathrm{ind}_3(4) = 4,\ \ \mathrm{ind}_3(5) = 5,\ \ \mathrm{ind}_3(6) = 3,$$

where it is understood that the arguments are defined modulo 7, and the outputs are defined modulo $\varphi(7) = 6$.

kth Roots in a Cyclic Group

The index is handy for understanding "kth roots" in a cyclic group G.

Let $G = \langle a \rangle$ have order m, and take any $b \in G$.

For any $k \in \mathbb{Z}$, consider the equation $x^k = b$ in G.

If we take the index on both sides we obtain

$$\operatorname{ind}_a(x^k) = k \operatorname{ind}_a(x) = \operatorname{ind}_a(b)$$

in $\mathbb{Z}/m\mathbb{Z}$. This is a linear congruence modulo m in the variable $y = \operatorname{ind}_a(x)$.

It follows that there are precisely (k, m) values of $\mathrm{ind}_a(x)$ modulo m iff $(k, m) \mid \mathrm{ind}_a(b)$. Thus:

Theorem 3

Let $G = \langle a \rangle$ be a cyclic group of order m, let $b \in G$ and let $k \in \mathbb{Z}$. The equation $x^k = b$ has precisely (k, m) solutions in G if and only if $(k, m) \mid \mathrm{ind}_a(b)$.

Example 1

Find all solutions of the congruence $x^{14} \equiv 133 \pmod{169}$.

Solution. The group $(\mathbb{Z}/169\mathbb{Z})^\times$ is cyclic of size $\varphi(169) = 13 \cdot 12 = 156$, with generator $2 + 169\mathbb{Z}$.

Computing the first few powers of 2 modulo 169 we quickly find

$$2^{16} \equiv 133 \pmod{169}.$$

Thus $\mathrm{ind}_2(133) = 16$.

Since $(14, 156) = 2$ divides 16, the congruence $x^{14} \equiv 133 \pmod{169}$ will have 2 incongruent solutions modulo 169.

To find them, we take the index on both sides and divide by 2:

$$14\,\mathrm{ind}_2(x) \equiv \mathrm{ind}_2(133) \equiv 16 \pmod{156} \;\Leftrightarrow\; 7\,\mathrm{ind}_2(x) \equiv 8 \pmod{78}.$$

Since $7 \cdot 11 = 77 \equiv -1 \pmod{78}$, multiplication by -11 yields

$$\mathrm{ind}_2(x) \equiv -88 \equiv 68 \pmod{78} \;\Leftrightarrow\; \mathrm{ind}_2(x) \equiv 68, 146 \pmod{156}.$$

Thus the solutions are $x = 2^{68}, 2^{146} \equiv 152, 17 \pmod{169}$. $\square$

Because of the inherent difficulty in computing discrete logarithms, Theorem 3 is of limited practical utility, even if a generator of G is given.

However if we modify our approach, we *can* extract an efficient means of at least determining whether or not the equation $x^k = b$ has a solution.

Notice that if G is abelian with order m and $x^k = b$, then

$$b^{m/(k,m)} = x^{km/(k,m)} = (x^m)^{k/(k,m)} = e^{k/(k,m)} = e.$$

If G is cyclic, the converse is also true!

Suppose that $G = \langle a \rangle$ has order m, $b \in G$, and $b^{m/(k,m)} = e$.

Then

$$0 + m\mathbb{Z} = \mathrm{ind}_a(e) = \mathrm{ind}_a(b^{m/(k,m)}) = \frac{m}{(k,m)}\,\mathrm{ind}_a(b).$$

So if $\mathrm{ind}_a(b) = \ell + m\mathbb{Z}$, then

$$\begin{aligned} \frac{m\ell}{(m,k)} \equiv 0 \pmod{m} \quad &\Leftrightarrow \quad m\ell \equiv 0 \pmod{m(m,k)} \\ &\Leftrightarrow \quad \ell \equiv 0 \pmod{(m,k)} \\ &\Leftrightarrow \quad \ell = rm + sk \end{aligned}$$

for some $r, s \in \mathbb{Z}$ (by Bézout's Lemma).

Thus

$$b = a^{\ell} = a^{rm+sk} = (a^m)^r (a^s)^k = e^r (a^s)^k = (a^s)^k,$$

so that $x^k = b$ has the solution $x = a^s$.

Let's summarize our findings:

Theorem 4

Let G be a cyclic group of order m, let $b \in G$ and let $k \in \mathbb{Z}$. The equation $x^k = b$ has a solution in G if and only if $b^{m/(k,m)} = e$.

From now on we will take $G = (\mathbb{Z}/n\mathbb{Z})^\times$ for some n with a primitive root.

Power Residues

Definition

Let $n, k \in \mathbb{N}$ and $a \in \mathbb{Z}$. We say that a is an *kth power residue of n* provided $(a, n) = 1$ and the congruence $x^k \equiv a \pmod{n}$ has a solution.

Applied to $G = (\mathbb{Z}/n\mathbb{Z})^\times$, Theorem 4 yields the following immediate corollary concerning power residues.

Corollary 1

Let $n \in \mathbb{N}$ have a primitive root modulo n, and suppose $a \in \mathbb{Z}$ satisfies $(a, n) = 1$. For any $k \in \mathbb{Z}$, a is a kth power residue of n if and only if $a^{\varphi(n)/(\varphi(n),k)} \equiv 1 \pmod{n}$.

Proof. Because it is cyclic, we can take $G = (\mathbb{Z}/n\mathbb{Z})^\times$, which has order $m = \varphi(n)$. $\square$

Example 2

Determine whether or not 193 is a 111th power residue of 298.

Solution. Since $298 = 2 \cdot 149$ and 149 is prime, primitive roots modulo 298 exist.

We have $\varphi(n) = \varphi(149) = 148 = 2^2 \cdot 37$ and $111 = 3 \cdot 37$ so that

$$\frac{\varphi(n)}{(\varphi(n), 111)} = \frac{2^2 \cdot 37}{37} = 4.$$

One can easily show that $193^4 \equiv 1 \pmod{298}$. So, by Corollary 1, the congruence $x^{111} \equiv 193 \pmod{298}$ must have a solution. $\square$

Power Residues of Primes

Because primitive roots modulo primes always exist, Corollary 1 implies:

Corollary 2

Let $p \in \mathbb{N}$ be prime and suppose $a \in \mathbb{Z}$ satisfies $p \nmid a$. For any $k \in \mathbb{Z}$, a is a kth power residue of p if and only if

$$a^{(p-1)/(p-1,k)} \equiv 1 \pmod{p}.$$

Proof. Since $\varphi(p) = p - 1$ and $(a, p) = 1$ iff $p \nmid a$, the result follows from Corollary 1. $\square$

When $k \in \mathbb{N}$ is small, we will refer to kth power residues as *quadratic residues*, *cubic residues*, *quartic residues*, etc.

An integer that is not a kth power residue will be called a kth power *nonresidue*.

From now on we will primarily be interested in quadratic residues modulo (odd) primes.

Because $(p-1, 2) = 2$ when p is odd, in this case Corollary 2 becomes:

Corollary 3 (Euler's Criterion)

Let $p \in \mathbb{N}$ be an odd prime and suppose $a \in \mathbb{Z}$ satisfies $p \nmid a$. Then a is a quadratic residue of p if and only if

$$a^{(p-1)/2} \equiv 1 \pmod{p}.$$

Example 3

Show that 2 and 7 are quadratic residues of $p = 457$, but that 5 is not.

Solution. We have $\frac{p-1}{2} = 228$ and repeated squaring gives

$$2^{228} \equiv 7^{228} \equiv 1 \pmod{457},$$

while

$$5^{228} \equiv 456 \equiv -1 \pmod{457}.$$

Now apply Euler's criterion. □

$\sqrt{-1}$ Modulo p (Again)

Let p be an odd prime.

Since

$$(-1)^{(p-1)/2} = 1 \;\Leftrightarrow\; \frac{p-1}{2} \equiv 0 \pmod 2 \;\Leftrightarrow\; p-1 \equiv 0 \pmod 4,$$

Euler's criterion tells us that -1 is a quadratic residue of p if and only if $p \equiv 1 \pmod 4$.

We deduced this earlier as a consequence of Wilson's Theorem.

Quadratic Congruences

Let p be an odd prime and consider the *quadratic congruence*

$$ax^2 + bx + c \equiv 0 \pmod{p}, \tag{1}$$

where $a, b, c \in \mathbb{Z}$ and $p \nmid a$, which has *discriminant* $\Delta = b^2 - 4ac$.

Theorem 5

Let p be an odd prime. If $p \nmid a$, the quadratic congruence (1) has solutions iff $p | \Delta$ or Δ is a quadratic residue of p. In this case, the solutions are given by the quadratic formula

$$x \equiv \frac{-b \pm \sqrt{\Delta}}{2a} \pmod{p},$$

where $\sqrt{\Delta}$ denotes any solution to $x^2 \equiv \Delta \pmod{p}$.

Proof

We follow the usual proof of the quadratic formula: complete the square and solve for x.

Suppose $x = r$ solves $ax^2 + bx + c \equiv 0 \pmod{p}$.

Because $p \nmid 2$, we can find $s \in \mathbb{Z}$ so that $2s \equiv 1 \pmod{p}$.

Likewise, we can find $t \in \mathbb{Z}$ so that $at \equiv 1 \pmod{p}$.

We then have

$$\begin{aligned} ar^2 + br + c \equiv 0 \pmod{p} &\Leftrightarrow t(ar^2 + br + c) \equiv 0 \pmod{p} \\ &\Leftrightarrow r^2 + btr + ct \equiv 0 \pmod{p} \\ &\Leftrightarrow (r + bst)^2 + ct - b^2s^2t^2 \equiv 0 \pmod{p} \end{aligned}$$

Thus, if the quadratic congruence has a solution, then

$$(r+bst)^2 \equiv b^2s^2t^2 - ct \equiv b^2s^2t^2 - 4cas^2t^2 \equiv s^2t^2\Delta \pmod{p}.$$

Multiplying through by $(2a)^2$ this becomes

$$(2ar+b)^2 \equiv \Delta \pmod{p}.$$

Thus either $p|\Delta$ or Δ is a quadratic residue of p.

Suppose that $d^2 \equiv \Delta \pmod{p}$. Then

$$\begin{aligned}(2ar+b)^2 - d^2 = ((2ar+b)-d)((2ar+b)+d) &\equiv 0 \pmod{p} \\ \Leftrightarrow\ 2ar+b &\equiv \pm d \pmod{p},\end{aligned}$$

since p is prime.

It now follows that $2ar \equiv -b \pm d \pmod{p}$, and multiplication by st yields

$$r \equiv st(-b \pm d) \equiv \frac{-b \pm \sqrt{\Delta}}{2a} \pmod{p},$$

since $s \equiv 2^{-1} \pmod{p}$ and $t \equiv a^{-1} \pmod{p}$. This proves one implication and establishes the quadratic formula.
For the converse, suppose that $\Delta \equiv d^2 \pmod{p}$ and set

$$r \equiv st(-b \pm d) \pmod{p}.$$

Reversing our steps above yields

$$(2ar + b)^2 \equiv d^2 \equiv \Delta \equiv b^2 - 4ac \pmod{p}.$$

Expanding the LHS and moving everything to the left we obtain

$$0 \equiv 4a^2r^2 + 4abr + 4ac \equiv 4a(ar^2 + br + c) \pmod{p}.$$

Since $p \nmid 4a$ and p is prime, this implies

$$ar^2 + br + c \equiv 0 \pmod{p},$$

which proves that r solves the quadratic congruence. $\square$

Example 4

Solve the quadratic congruence $11x^2 + 6x + 1 \equiv 0 \pmod{19}$.

Solution. We have

$$\Delta = 6^2 - 4 \cdot 11 \cdot 1 = -8 \pmod{19}.$$

By Fermat's Little Theorem we have

$$\begin{aligned}\Delta^{(19-1)/2} &= \Delta^9 \equiv (-8)^9 \equiv -2^{27} \equiv -2^9 \pmod{19}\\ &\equiv -2 \cdot 16 \cdot 16 \equiv (-2)(-3)(-3) \equiv -18 \equiv 1 \pmod{19}.\end{aligned}$$

According to Euler's criterion Δ is therefore a quadratic residue of 19.

Thus the quadratic congruence has exactly two solutions modulo 19, given by the quadratic formula.

Since $4 \cdot 19 = 76 = 7 \cdot 11 - 1$, $11^{-1} \equiv 7 \pmod{19}$.

Since $2 \cdot 10 = 20 \equiv 1 \pmod{19}$, $2^{-1} \equiv 10 \pmod{19}$.

And since $19 + 17 = 6^2$, we have

$$2^2 \cdot 6^2 \equiv 2^2 \cdot 17 \equiv 2^2(-2) \equiv \Delta \pmod{19},$$

so that $\sqrt{\Delta} \equiv 12 \pmod{19}$.

Finally, the quadratic formula yields

$$x \equiv 7 \cdot 10 \cdot (-6 \pm 12) \equiv -6(-18), -6(6) \equiv -6, 2 \equiv 2, 13 \pmod{19}.$$

$\square$

Example 5

Solve the quadratic congruence $x^2 + x + 1 \equiv 0 \pmod{91}$.

Solution. Since $91 = 7 \cdot 13$, the CRT implies that the given congruence is equivalent to the system

$$x^2 + x + 1 \equiv 0 \pmod{7},$$
$$x^2 + x + 1 \equiv 0 \pmod{13}.$$

The discriminant is $\Delta = -3$, and we have

$$(-3)^{(7-1)/2} = (-3)^3 = -27 \equiv 1 \pmod 7,$$
$$(-3)^{(13-1)/2} = (-3)^6 = 27^2 \equiv 1^2 \equiv 1 \pmod{13}.$$

Euler's criterion then implies that Δ is a quadratic residue of both 7 and 13, so that the congruences making up our system have two solutions each.
The quadratic formula yields the solutions

$$x \equiv 2, 4 \pmod 7,$$
$$x \equiv 3, 9 \pmod{13}.$$

Piecing these back together in pairs using the CRT we arrive at the overall solutions

$$x \equiv 9, 16, 81, 64 \pmod{91}.$$

□