# Applications of Modular Arithmetic

## A Proof of Quadratic Reciprocity

Michael Gintz and Zack Stier

Princeton University

15 August 2019

# Modular Arithmetic

Modular arithmetic involves performing operations on integers **modulo n**.

# Modular Arithmetic

Modular arithmetic involves performing operations on integers **modulo n**. Two integers are **equivalent modulo n** if they differ by a multiple of $n$.

# Modular Arithmetic

Modular arithmetic involves performing operations on integers **modulo n**.
Two integers are **equivalent modulo n** if they differ by a multiple of *n*.

$$17^2 - 8 \times 25 \equiv \quad \pmod{10}$$

# Modular Arithmetic

Modular arithmetic involves performing operations on integers **modulo n**. Two integers are **equivalent modulo n** if they differ by a multiple of *n*.

$$17^2 - 8 \times 25 \equiv 9 \pmod{10}$$

**Problem (2015 PUMaC NT A1)**

*What is the 22nd positive integer $n$ such that $22^n$ ends in a 2? (when written in base 10)*

*Solution:* The powers of 22, modulo 10, are 2, 4, 8, 6, 2, . . . . Thus the last digit is a 2 when $n$ is 1, 5, 9, etc. The 22nd term in this sequence is $\boxed{85}$.

**Problem (2015 PUMaC NT A1)**

*What is the 22nd positive integer $n$ such that $22^n$ ends in a 2? (when written in base 10)*

*Solution:* The powers of 22, modulo 10, are 2, 4, 8, 6, 2, . . . . Thus the last digit is a 2 when $n$ is 1, 5, 9, etc. The 22nd term in this sequence is $\boxed{85}$.

*See also: 2011 NT A3, 2013 NT A2, 2014 NT A2, 2015 NT B1, 2016 NT A4, 2016 NT A7, 2016 NT A8, 2017 NT A6, 2018 NT A1, 2018 NT A5,*

# Chinese Remainder Theorem

**Theorem (Chinese Remainder Theorem)**

*If* $a_1$ *and* $a_1$ *are coprime and*

$$n \equiv b_1 \pmod{a_1}$$
$$n \equiv b_2 \pmod{a_2}$$

*then there is a unique* $b$ *with*

$$n \equiv b \pmod{a_1 a_2}.$$

# Chinese Remainder Theorem

**Theorem (Chinese Remainder Theorem)**

*If* $a_1$ *and* $a_1$ *are coprime and*

$$n \equiv b_1 \pmod{a_1}$$
$$n \equiv b_2 \pmod{a_2}$$

*then there is a unique* $b$ *with*

$$n \equiv b \pmod{a_1 a_2}.$$

**Remark:** If $c_1 = c_2 = 0$ then $c = 0$.

# Chinese Remainder Theorem

**Theorem (Chinese Remainder Theorem)**

*If* $a_1$ *and* $a_1$ *are coprime and*

$$n \equiv b_1 \pmod{a_1}$$
$$n \equiv b_2 \pmod{a_2}$$

*then there is a unique* $b$ *with*

$$n \equiv b \pmod{a_1 a_2}.$$

**Remark:** If $c_1 = c_2 = 0$ then $c = 0$.
**Remark:** This fact is also true with $a_1, \ldots, a_k$ and $b_1, \ldots, b_k$.

**Problem (2012 PUMaC NT A1)**

*Albert has a bag of candies that he want to share with his friends. At first, he splits the candies evenly amongst 20 friends and himself and he finds that there are five left over. Ante arrives, and they redistribute the candies evenly again among the 22 people. This time, there are three left over. If the bag contains over 500 candies, what is the fewest possible number of candies?*

# Chinese Remainder Theorem

**Problem (2012 PUMaC NT A1)**

*Albert has a bag of candies that he want to share with his friends. At first, he splits the candies evenly amongst 20 friends and himself and he finds that there are five left over. Ante arrives, and they redistribute the candies evenly again among the 22 people. This time, there are three left over. If the bag contains over 500 candies, what is the fewest possible number of candies?*

*Solution:* Let $x$ be the answer. It is the case that

$$\begin{aligned} x &\equiv 3 \pmod{21} \\ x &\equiv 5 \pmod{22} \\ \implies x &\equiv 47 \pmod{21 \times 22} \end{aligned}$$

so $\boxed{x = 509}$.

# Chinese Remainder Theorem

## Problem (2012 PUMaC NT A1)

*Albert has a bag of candies that he want to share with his friends. At first, he splits the candies evenly amongst 20 friends and himself and he finds that there are five left over. Ante arrives, and they redistribute the candies evenly again among the 22 people. This time, there are three left over. If the bag contains over 500 candies, what is the fewest possible number of candies?*

*Solution:* Let $x$ be the answer. It is the case that

$$\begin{aligned} x &\equiv 3 \pmod{21} \\ x &\equiv 5 \pmod{22} \\ \Longrightarrow \quad x &\equiv 47 \pmod{21 \times 22} \end{aligned}$$

so $\boxed{x = 509}$.

*See also: 2010 NT A7*

# Powers Modulo a Prime

Consider the powers of 3 mod 7. We have

$$3^1 \equiv 3 \quad 3^2 \equiv 2 \quad 3^3 \equiv 6 \quad 3^4 \equiv 4 \quad 3^5 \equiv 5 \quad 3^6 \equiv 1 \pmod 7$$

# Powers Modulo a Prime

Consider the powers of 3 mod 7. We have

$$3^1 \equiv 3 \quad 3^2 \equiv 2 \quad 3^3 \equiv 6 \quad 3^4 \equiv 4 \quad 3^5 \equiv 5 \quad 3^6 \equiv 1 \pmod 7$$

Before we consider when we arrive at every nonzero value modulo a prime, let us first note when powers of a number are equivalent to 1 modulo another number.

**Definition**

Let $n$ be a positive integer. Then $\varphi(n)$ is the number of integers at most $n$ which are relatively prime to $n$.

# Powers Modulo a Prime

Consider the powers of 3 mod 7. We have

$$3^1 \equiv 3 \quad 3^2 \equiv 2 \quad 3^3 \equiv 6 \quad 3^4 \equiv 4 \quad 3^5 \equiv 5 \quad 3^6 \equiv 1 \pmod 7$$

Before we consider when we arrive at every nonzero value modulo a prime, let us first note when powers of a number are equivalent to 1 modulo another number.

**Definition**

Let $n$ be a positive integer. Then $\varphi(n)$ is the number of integers at most $n$ which are relatively prime to $n$.

*See also: 2010 NT A4, 2013 NT A4*

# Euler's Theorem

**Theorem (Euler's Theorem)**

*For coprime $a, b$ we have $a^{\varphi(b)} \equiv 1 \pmod{b}$.*

*Proof:* Say $k_1, \ldots, k_{\varphi(b)}$ are the values less than $b$ relatively prime to $b$. Then

$$k_1 \times k_2 \times \ldots \times k_{\varphi(b)} \equiv ak_1 \times ak_2 \times \ldots \times ak_{\varphi(b)} \pmod{b}$$
$$k_1 \times k_2 \times \ldots \times k_{\varphi(b)} \equiv a^{\varphi(b)}(k_1 \times k_2 \times \ldots \times k_{\varphi(b)}) \pmod{b}$$
$$1 \equiv a^{\varphi(b)} \pmod{b}.$$

# Fermat's Little Theorem

**Theorem (Fermat's Little Theorem)**

*For any prime $p$ and positive integer $a$ not a multiple of $p$, $a^{p-1} \equiv 1 \pmod{p}$.*

*Proof:* $\varphi(p) = p - 1$, so we use Euler's Theorem.

**Problem (PUMaC 2015 NT A4)**

*What is the smallest positive integer n such that* $20 \equiv n^{15} \pmod{29}$*?*

*Solution:* Let $a$ be the answer. $29 \nmid a$, so $a^{28} \equiv 1 \pmod{29}$.

**Problem (PUMaC 2015 NT A4)**

*What is the smallest positive integer n such that* $20 \equiv n^{15} \pmod{29}$*?*

*Solution:* Let $a$ be the answer. $29 \nmid a$, so $a^{28} \equiv 1 \pmod{29}$. Then, $a^{14} \equiv \pm 1$, so $a^{15} \equiv \pm a$. Therefore $a \equiv -20, 20 \pmod{29}$.

## Problem (PUMaC 2015 NT A4)

*What is the smallest positive integer n such that* $20 \equiv n^{15} \pmod{29}$*?*

*Solution:* Let $a$ be the answer. $29 \nmid a$, so $a^{28} \equiv 1 \pmod{29}$. Then, $a^{14} \equiv \pm 1$, so $a^{15} \equiv \pm a$. Therefore $a \equiv -20, 20 \pmod{29}$. The first candidate is $a = 9$, which does not work (by computation). The next candidate is $\boxed{a = 20}$, which does work (by computation).

**Problem (PUMaC 2015 NT A4)**

*What is the smallest positive integer n such that* $20 \equiv n^{15} \pmod{29}$*?*

*Solution:* Let $a$ be the answer. $29 \nmid a$, so $a^{28} \equiv 1 \pmod{29}$. Then, $a^{14} \equiv \pm 1$, so $a^{15} \equiv \pm a$. Therefore $a \equiv -20, 20 \pmod{29}$. The first candidate is $a = 9$, which does not work (by computation). The next candidate is $\boxed{a = 20}$, which does work (by computation).
*See also: 2011 NT A1, 2012 NT A7, 2015 NT A5, 2016 NT A6, 2017 T10*

# Primitive Roots

Now that we know that the number of terms we see in powers modulo a prime is $p - 1$, we might ask whether there must exist a term whose powers make up every nonzero modulus? We can prove this in two parts.

# Primitive Roots

Now that we know that the number of terms we see in powers modulo a prime is $p-1$, we might ask whether there must exist a term whose powers make up every nonzero modulus? We can prove this in two parts.

**Definition**

The **order** of $a \pmod p$ is the smallest $o$ such that $a^o \equiv 1 \pmod p$.

Note that the order must divide $\varphi(p)$.

# Primitive Roots

Now that we know that the number of terms we see in powers modulo a prime is $p-1$, we might ask whether there must exist a term whose powers make up every nonzero modulus? We can prove this in two parts.

**Definition**

The **order** of $a \pmod{p}$ is the smallest $o$ such that $a^o \equiv 1 \pmod{p}$.

Note that the order must divide $\varphi(p)$.

**Theorem**

*The number of values modulo p which have order o is at most $\varphi(o)$.*

# Primitive Roots

Now that we know that the number of terms we see in powers modulo a prime is $p-1$, we might ask whether there must exist a term whose powers make up every nonzero modulus? We can prove this in two parts.

**Definition**

The **order** of $a \pmod{p}$ is the smallest $o$ such that $a^o \equiv 1 \pmod{p}$.

Note that the order must divide $\varphi(p)$.

**Theorem**

*The number of values modulo p which have order o is at most $\varphi(o)$.*

*Proof:* Note that these are all solutions to $x^o \equiv 1 \pmod{p}$. We can factor the solutions from this, showing that there are at most $o$ solutions. Then at most $\varphi(o)$ solutions, because if there is one solution, then any power of this not coprime with $o$ will also be a solution, but won't have order $o$.

*See also: 2015 NT A7*

# Primitive Roots

**Theorem**

*For all positive integers n we have*

$$n = \sum_{d|n} \varphi(d)$$

# Primitive Roots

**Theorem**

*For all positive integers n we have*

$$n = \sum_{d|n} \varphi(d)$$

*Proof:* There are $\varphi(d)$ values whose gcd with $n$ is $n/d$, and each value corresponds to one of these.

# Primitive Roots

**Theorem**

*For all positive integers $n$ we have*

$$n = \sum_{d|n} \varphi(d)$$

*Proof:* There are $\varphi(d)$ values whose gcd with $n$ is $n/d$, and each value corresponds to one of these. By combining these, we see that there are exactly $\varphi(d)$ values of order $d$ for all $d|n$, and thus there are $\varphi(p-1)$ primitive roots for any prime $p$.

# Quadratic Residues

A **quadratic residue modulo n** is a value which is equivalent to a square number modulo **n**.
The quadratic residues modulo 7 are $0, 1, 2, 4$ (these are the only things equivalent to one of $1^2, 3^2, \ldots, 7^2$).

**Problem (2012 PUMaC NT A2)**

*How many ways can $2^{2012}$ be expressed as the sum of four (not necessarily distinct) positive squares?*

*Solution:* Say $a^2 + b^2 + c^2 + d^2 = 2^{2012}$.

**Problem (2012 PUMaC NT A2)**

*How many ways can $2^{2012}$ be expressed as the sum of four (not necessarily distinct) positive squares?*

*Solution:* Say $a^2 + b^2 + c^2 + d^2 = 2^{2012}$. Looking modulo 4, $a$, $b$, $c$, and $d$ must all be all even or all odd, since the residues are 0 or 1, respectively.

**Problem (2012 PUMaC NT A2)**

*How many ways can $2^{2012}$ be expressed as the sum of four (not necessarily distinct) positive squares?*

*Solution:* Say $a^2 + b^2 + c^2 + d^2 = 2^{2012}$. Looking modulo 4, $a$, $b$, $c$, and $d$ must all be all even or all odd, since the residues are 0 or 1, respectively. However, looking modulo 8, $2^{2012} \equiv 0$, so they cannot be all odd.

**Problem (2012 PUMaC NT A2)**

*How many ways can $2^{2012}$ be expressed as the sum of four (not necessarily distinct) positive squares?*

*Solution:* Say $a^2 + b^2 + c^2 + d^2 = 2^{2012}$. Looking modulo 4, $a$, $b$, $c$, and $d$ must all be all even or all odd, since the residues are 0 or 1, respectively. However, looking modulo 8, $2^{2012} \equiv 0$, so they cannot be all odd. Therefore, they are all even. We divide by 4 and repeat, finding $a^2 + b^2 + c^2 + d^2 = 4$,

**Problem (2012 PUMaC NT A2)**

*How many ways can $2^{2012}$ be expressed as the sum of four (not necessarily distinct) positive squares?*

*Solution:* Say $a^2 + b^2 + c^2 + d^2 = 2^{2012}$. Looking modulo 4, $a$, $b$, $c$, and $d$ must all be all even or all odd, since the residues are 0 or 1, respectively. However, looking modulo 8, $2^{2012} \equiv 0$, so they cannot be all odd. Therefore, they are all even. We divide by 4 and repeat, finding $a^2 + b^2 + c^2 + d^2 = 4$, so the answer is 1.

*See also: 2012 NT A4, 2017 NT A5, 2017 NT A7, 2018 NT A6, 2018 T4*

# Quadratic Residues

## Definition

Let $a$ be an integer and let $p$ be an odd prime. Then the **Legendre symbol** $(a/p)$ is equal to:

- 0 if $p \mid a$,
- 1 if $p \nmid a$ and $a \equiv b^2 \pmod{p}$ for some $b$, and
- $-1$ otherwise.

# Calculating Quadratic Residues

In order to calculate Legendre symbols, it is useful to define some equivalences:

**Definition**

If $a$ is an integer and $b = p_1 \times \ldots \times p_k$ is an odd integer, then the **Jacobi symbol** $(a/b)$ is equal to $(a/p_1) \times \ldots \times (a/p_k)$.

# Calculating Quadratic Residues

In order to calculate Legendre symbols, it is useful to define some equivalences:

**Definition**

If $a$ is an integer and $b = p_1 \times \ldots \times p_k$ is an odd integer, then the **Jacobi symbol** $(a/b)$ is equal to $(a/p_1) \times \ldots \times (a/p_k)$.

We have the following equivalences:

- $(a/b) = (a - kb/b)$

# Calculating Quadratic Residues

In order to calculate Legendre symbols, it is useful to define some equivalences:

**Definition**

If $a$ is an integer and $b = p_1 \times \ldots \times p_k$ is an odd integer, then the **Jacobi symbol** $(a/b)$ is equal to $(a/p_1) \times \ldots \times (a/p_k)$.

We have the following equivalences:

- $(a/b) = (a - kb/b)$
- $(ab/c) = (a/c)(b/c)$

# Calculating Quadratic Residues

In order to calculate Legendre symbols, it is useful to define some equivalences:

**Definition**

If $a$ is an integer and $b = p_1 \times \ldots \times p_k$ is an odd integer, then the **Jacobi symbol** $(a/b)$ is equal to $(a/p_1) \times \ldots \times (a/p_k)$.

We have the following equivalences:

- $(a/b) = (a - kb/b)$
- $(ab/c) = (a/c)(b/c)$
- $(a/bc) = (a/b)(a/c)$

# Calculating Quadratic Residues

In order to calculate Legendre symbols, it is useful to define some equivalences:

**Definition**

If $a$ is an integer and $b = p_1 \times \ldots \times p_k$ is an odd integer, then the **Jacobi symbol** $(a/b)$ is equal to $(a/p_1) \times \ldots \times (a/p_k)$.

We have the following equivalences:

- $(a/b) = (a - kb/b)$
- $(ab/c) = (a/c)(b/c)$
- $(a/bc) = (a/b)(a/c)$

From these, if we can determine $(2/p)$ and $(q/p)$ in terms of $(p/q)$ when $p$ and $q$ are primes, then we can determine the value of $(p/q)$ for all primes $q$.

# Quadratic Reciprocity

**Theorem (Quadratic Reciprocity)**

*Say $p$ and $q$ are odd primes. Then $(p/q) = (q/p)$ if either $p$ or $q$ are equivalent to $1 \pmod 4$, and $(p/q) = -(q/p)$ otherwise.*

# Quadratic Reciprocity

**Theorem (Quadratic Reciprocity)**

*Say $p$ and $q$ are odd primes. Then $(p/q) = (q/p)$ if either $p$ or $q$ are equivalent to $1 \pmod 4$, and $(p/q) = -(q/p)$ otherwise.*

In order to prove this, we first want to see if we can rewrite our Legendre symbol:

**Theorem**

*For positive integers $a$ and primes $p$, then $(a/p) \equiv a^{(p-1)/2} \pmod p$.*

# Quadratic Reciprocity

**Theorem (Quadratic Reciprocity)**

*Say $p$ and $q$ are odd primes. Then $(p/q) = (q/p)$ if either $p$ or $q$ are equivalent to $1 \pmod 4$, and $(p/q) = -(q/p)$ otherwise.*

In order to prove this, we first want to see if we can rewrite our Legendre symbol:

**Theorem**

*For positive integers $a$ and primes $p$, then $(a/p) \equiv a^{(p-1)/2} \pmod p$.*

*Proof:* If $a$ is a multiple of $p$, this is trivial. Otherwise, write $a$ as a power of a primitive root, and note that the power is even if and only if $a$ is a quadratic residue.

# Gauss' Criterion

Let's define the **even-remainder** function $e(a, p)$ as follows:

- Take the odd multiples of $a$ less than $ap$: $a, 3a, \ldots, (p-2)a$.
- Find the remainders when these are divided by $p$, and call them $s_1, s_2, \ldots, s_{(p-1)/2}$.
- Then we say that $e(a, p)$ is the number of even values of $s_i$.

# Gauss' Criterion

Let's define the **even-remainder** function $e(a,p)$ as follows:

- Take the odd multiples of $a$ less than $ap$: $a, 3a, \ldots, (p-2)a$.
- Find the remainders when these are divided by $p$, and call them $s_1, s_2, \ldots, s_{(p-1)/2}$.
- Then we say that $e(a,p)$ is the number of even values of $s_i$.

**Theorem**

*For all positive integers a and primes p, we have* $(a/p) = (-1)^{e(a,p)}$.

To show that this is true, we will use an argument similar to the one we used before:

- Multiply each element of a set of numbers by a constant,
- Factor the original set out of the result modulo $p$.

# Proving Gauss' Criterion

*Proof:* Consider the set where we replace even values $s_i$ with $p - s_i$. Note that then we have $(p-1)/2$ odd values.

# Proving Gauss' Criterion

*Proof:* Consider the set where we replace even values $s_i$ with $p - s_i$. Note that then we have $(p-1)/2$ odd values.
The values that were originally the same parity are distinct, and if two values were originally different parity, then their difference modulo $p$ is the sum of two even multiples of $a$ less than $pa$, so they cannot differ by a multiple of $p$.

# Proving Gauss' Criterion

*Proof:* Consider the set where we replace even values $s_i$ with $p - s_i$. Note that then we have $(p-1)/2$ odd values.
The values that were originally the same parity are distinct, and if two values were originally different parity, then their difference modulo $p$ is the sum of two even multiples of $a$ less than $pa$, so they cannot differ by a multiple of $p$.
Then

$$1 \times 3 \times \ldots \times p - 2 \equiv a^{(p-1)/2}(-1)^{e(a,p)}(1 \times 3 \times \ldots \times p - 2) \pmod{p}$$
$$1 \equiv a^{(p-1)/2}(-1)^{e(a,p)} \pmod{p}$$

# Proving Gauss' Criterion

*Proof:* Consider the set where we replace even values $s_i$ with $p - s_i$. Note that then we have $(p-1)/2$ odd values.
The values that were originally the same parity are distinct, and if two values were originally different parity, then their difference modulo $p$ is the sum of two even multiples of $a$ less than $pa$, so they cannot differ by a multiple of $p$.
Then

$$1 \times 3 \times \ldots \times p - 2 \equiv a^{(p-1)/2}(-1)^{e(a,p)}(1 \times 3 \times \ldots \times p - 2) \pmod{p}$$
$$1 \equiv a^{(p-1)/2}(-1)^{e(a,p)} \pmod{p}$$

Since both of these are equivalent to either 1 or $-1$, we are done.

# Proving Quadratic Reciprocity

Let's take another look at the statement:

**Theorem (Quadratic Reciprocity)**

*Say $p$ and $q$ are odd primes. Then $(p/q) = (q/p)$ if either $p$ or $q$ are equivalent to $1 \pmod 4$, and $(p/q) = -(q/p)$ otherwise.*

# Proving Quadratic Reciprocity

Let's take another look at the statement:

**Theorem (Quadratic Reciprocity)**

*Say $p$ and $q$ are odd primes. Then $(p/q) = (q/p)$ if either $p$ or $q$ are equivalent to $1 \pmod 4$, and $(p/q) = -(q/p)$ otherwise.*

*Proof:* We will prove that $(p/q)(q/p)$ is 1 when one of these is 1 modulo 4, and $-1$ otherwise. Note that from Gauss' Criterion, this product equals $(-1)^{e(p,q)+e(q,p)}$.

# Proving Quadratic Reciprocity

Let's take another look at the statement:

**Theorem (Quadratic Reciprocity)**

*Say $p$ and $q$ are odd primes. Then $(p/q) = (q/p)$ if either $p$ or $q$ are equivalent to $1 \pmod 4$, and $(p/q) = -(q/p)$ otherwise.*

*Proof:* We will prove that $(p/q)(q/p)$ is 1 when one of these is 1 modulo 4, and $-1$ otherwise. Note that from Gauss' Criterion, this product equals $(-1)^{e(p,q)+e(q,p)}$.

There is a bijection between $e(p,q)$ and pairs of positive odd $(a,b)$ such that $a < q$, $b < p$ and $0 < ap - bq < p$ is even.

# Proving Quadratic Reciprocity

Let's take another look at the statement:

**Theorem (Quadratic Reciprocity)**

*Say p and q are odd primes. Then $(p/q) = (q/p)$ if either p or q are equivalent to $1 \pmod 4$, and $(p/q) = -(q/p)$ otherwise.*

*Proof:* We will prove that $(p/q)(q/p)$ is 1 when one of these is 1 modulo 4, and $-1$ otherwise. Note that from Gauss' Criterion, this product equals $(-1)^{e(p,q)+e(q,p)}$.

There is a bijection between $e(p, q)$ and pairs of positive odd $(a, b)$ such that $a < q$, $b < p$ and $0 < ap - bq < p$ is even.

There is a bijection between $e(q, p)$ and pairs of positive odd $(a, b)$ such that $a < q$, $b < p$ and $0 < bq - ap < q$ is even. We can write this as $-p < ap - bq < 0$.

# Proving Quadratic Reciprocity

Since there are no such values which give us 0, there is a bijection between $e(p, q) + e(q, p)$ and positive odd $a < q, b < p$ such that $-p < ap - bq < q$.

# Proving Quadratic Reciprocity

Since there are no such values which give us 0, there is a bijection between $e(p, q) + e(q, p)$ and positive odd $a < q, b < p$ such that
$-p < ap - bq < q$.
If $(a, b)$ is a solution, then so is $(q - 1 - a, p - 1 - b)$, and if $a, b$ are both equivalent to 3 modulo 4 then $((q - 1)/2, (p - 1)/2)$ is a solution. And we're done!