# Math Circles: Primality Testing and Integer Factorization

Owen Sharpe

University of Waterloo

March 27, 2024

# Recap

Last time we discussed the following topics:

- Properties of prime numbers.
- Techniques for factoring positive integers.
- Techniques for creating lists of primes.
- Approximating the number of primes up to $x$.

# Division Algorithm

**Theorem (Division Algorithm)**

*Let $a$ be an integer and $b$ a positive integer. Then there exist unique integers $q, r$ with $0 \leq r < b$ such that $a = bq + r$.*

In the previous theorem, $q$ is the integer part of $a/b$ and $r$ is the remainder. We will use the notation $a \mathbin{\%} b$ to denote the remainder of $a$ upon division by $b$. Arithmetic with remainders is an important tool in number theory.

# Remainder Arithmetic

**Example**

We calculate that $26 \% 10 = 6$ and $39 \% 10 = 9$. Notice that

$$(26 + 39) \% 10 = 65 \% 10 = 5,$$

$$(6 + 9) \% 10 = 15 \% 10 = 5,$$

and that

$$(26 \times 39) \% 10 = 1014 \% 10 = 4,$$

$$(6 \times 9) \% 10 = 54 \% 10 = 4.$$

This is not a coincidence.

# Congruence Mod $m$

We can formally state a result about how remainders behave with addition and multiplication once we define the notion of congruence.

**Definition (Congruence Mod $m$)**

For integers $a, b$ and a positive integer $m$, we say that

$$a \equiv b \pmod{m}$$

($a$ is congruent to $b$ mod $m$) if

- $a \,\%\, m = b \,\%\, m$
- or equivalently $b = a + qm$ for some integer $q$
- or equivalently $m \mid a - b$ ($m$ divides $a - b$).

The first condition implies that $a$ is congruent to its remainder mod $m$. The last condition is usually the easiest to calculate with.

# Congruence Mod $m$

## Example

- $17 \equiv 35 \pmod 6$ because $6 \mid 17 - 35 = -18$
- $-2 \equiv 6 \pmod 4$ because $4 \mid -2 - 6 = 8$
- $2 \not\equiv 7 \pmod 9$ because $9 \nmid 2 - 7 = -5$.

## Exercise

*Determine whether the following statements are true.*

- $16 \equiv 51 \pmod 5$
- $21 \equiv 0 \pmod 7$
- $4 \equiv 12 \pmod{16}$
- $-4 \equiv 12 \pmod{16}$

# Congruence Class Mod $m$

## Definition

Fix a positive integer $m$ and an integer $a$. The congruence class of $a$ mod $m$, sometimes written $[a]$, is the set of integers congruent to $a$ mod $m$.

## Example

The congruence class of 17 mod 5 is the infinite set

$$\{\ldots, -13, -8, -3, 2, 7, 12, 17, 22, \ldots\}.$$

## Exercise

*Determine whether the following equalities are true:*

- $[-4] = [16] \pmod 5$
- $[2] = [14] \pmod 7$.

# Modular Arithmetic

Now we state the result alluded to earlier about addition and multiplication of remainders.

## Proposition

*Fix integers $a, b, c$ and a positive integer $m$. Suppose $a \equiv b \pmod{m}$. Then $a + c \equiv b + c \pmod{m}$ and $ac \equiv bc \pmod{m}$.*

# Modular Arithmetic

**Proof.**

If $a \equiv b \pmod{m}$, then $a = qm + b$ for some integer $q$. Then

$$a + c = (qm + b) + c = qm + (b + c)$$

and

$$ac = (qm + b)c = (qc)m + bc,$$

implying that $a + c \equiv b + c \pmod{m}$ and $ac \equiv bc \pmod{m}$ as desired. □

# Modular Arithmetic

We have just seen that two integers behave *exactly* the same with addition and subtraction mod $m$ if they are congruent mod $m$. This allows us to define arithmetic on congruence classes via the rule $[a] + [b] = [a + b]$ and $[a][b] = [ab]$.

### Example

Since $[26] = [6]$ and $[39] = [9]$ mod 10, we can safely assume that

$$[26] + [39] = [6] + [9] = [6 + 9] = [15] = [5]$$

and

$$[26][39] = [6][9] = [6 \times 9] = [54] = [4].$$

# Modular Arithmetic

## Example

Let's calculate $(20406 \times 987654321) \ \% \ 100$.

- Notice that $20406 \equiv 6 \pmod{100}$ and $987654321 \equiv 21 \pmod{100}$.
- Therefore $20406 \times 987654321 \equiv 6 \times 21 \equiv 126 \equiv 26 \pmod{100}$.
- Since $0 \leq 26 < 100$, the remainder is 26.

## Example

Let's calculate $4^{40404} \ \% \ 17$

- Notice that $4^2 \equiv 16 \equiv -1 \pmod{17}$.
- Therefore $4^{40404} \equiv 16^{20202} \equiv (-1)^{20202} \equiv 1 \pmod{17}$.
- Since $0 \leq 1 < 17$, the remainder is 1.

# Modular Arithmetic

**Exercise**

*Calculate* $7^{200}$ % 48.

**Exercise**

*Calculate* $11^{301}$ % 1332.

**Exercise**

*Calculate* $3^k$ % 10 , *for* $0 \leq k \leq 12$. *What do you notice?*

# Modular Arithmetic

## Example

Let's prove that $2^{3k} + 1$ is composite for any integer $k \geq 1$. Indeed,

$$2^{3k} + 1 \equiv (2^k)^3 + 1 \equiv (-1)^3 + 1 \equiv 0 \pmod{2^k + 1},$$

which implies that $2^{3k} + 1$ always has $2^k + 1$ as a factor.

## Exercise

*Show more generally that if $m \geq 1$ has any odd prime factor, that $2^m + 1$ is composite.*

## Exercise

*Show that if $m$ is composite, then $2^m - 1$ is composite.*

# Fermat Numbers

- If $2^m + 1$ is prime, then $m$ has no odd prime factors, i.e., $m$ is a power of 2.
- A Fermat number is a number of the form $F_m = 2^{2^m} + 1$.
- The Fermat numbers $F_0$ through $F_4$ are prime, but $F_5$ through $F_{32}$ are not.
- It is unknown whether there are infinitely many Fermat primes.

# Mersenne Numbers

- If $2^m - 1$ is prime, then $m$ is prime.
- A Mersenne number is a number of the form $M_p = 2^p - 1$ for a prime $p$.
- There are only 51 known primes $p$ such that $M_p$ is also prime.
- Every prime $p$ up to about 67 million has been tested to check if $M_p$ is prime.
- The largest known prime number is the Mersenne prime $2^{82589933} - 1$.
- It is unknown whether there are infinitely many Mersenne primes.

# Fermat's Little Theorem

## Theorem (Fermat's Little Theorem)

*Suppose $p$ is prime and $a$ is an integer not divisible by $p$. Then $a^{p-1} \equiv 1 \pmod{p}$.*

## Example

- We have $2^6 \equiv 64 \equiv 1 \pmod{7}$, since 7 is prime and $7 \nmid 2$ (2 does not divide 7).
- We have $2^8 \equiv 256 \equiv 4 \not\equiv 1 \pmod{9}$, and since $9 \nmid 2$, this proves that 9 is composite.

# Fermat Test

The Fermat test for primality of $m$ works as follows:

- Choose an integer $a$ (usually between 2 and $n-1$).
- If $a^{m-1} \not\equiv 1 \pmod{m}$, then $m$ is definitely composite.
- If $a^{m-1} \equiv 1 \pmod{m}$, then $m$ is "probably prime".

**Example**

Recall from last time that $10^8+1 = 17 \times 5882353$. Using a computer, we could calculate

$$2^{10^8+1} \equiv 65536 \pmod{10^8+1},$$

which immediately shows that $10^8+1$ is not prime. On the other hand,

$$2^{5882352} \equiv 1 \pmod{5882353},$$

which suggests that 5882353 is prime.

# Fermat Pseudoprimes

Unfortunately, $a^{m-1} \equiv 1 \pmod{m}$ may hold even if $m$ is composite in some cases. The only guarantee is that if $a$ and $m$ share a prime factor $q$, then $a^{m-1} \not\equiv 1 \pmod{m}$.

## Definition (Fermat Pseudoprime / Witness)

Fix a composite integer $m$.

- $m$ is said to be a Fermat pseudoprime base $a$ if $a^{m-1} \equiv 1 \pmod{m}$.
- An integer $a$ is said to be a Fermat witness to the compositeness of $m$ if $a^{m-1} \not\equiv 1 \pmod{m}$ and $a$ is not divisible by $m$.

## Definition (Carmichael Number)

A composite number $m$ is said to be a Carmichael number if it is a Fermat pseudoprime base $a$ for every integer $a$ coprime to $m$ (sharing no prime factors with $m$).

# Korselt's Criterion

We say that an integer is squarefree if its prime factorization contains no repeated factors (higher powers of primes). Korselt proved that a composite integer $m$ is a Carmichael number if and only if $m$ is squarefree and for each prime factor $p$ of $m$, $p - 1 \mid m - 1$.

**Exercise**

*Verify that* 561 *is a Carmichael number.*

# Fermat Test

The existence of Carmichael numbers makes the Fermat test an unsatisfactory test. The smallest witness to a Carmichael number $m$ would be the smallest prime factor of $m$, but then we may as well have used trial factorization. Better tests exist.

# Polynomials Mod $m$

Since we have defined addition and multiplication on congruence classes, we can also define polynomials on congruence classes.

## Example

Let's evaluate the polynomial $2x^3 + 3x \pmod{11}$ at the points $[x] = [2]$, $[x] = [3]$, and $[x] = [13]$. Directly substituting yields

$$2 \times 2^3 + 3 \times 2 \equiv 16 + 6 \equiv 7 \pmod{11},$$

$$3 \times 3^3 + 3 \times 3 \equiv 81 + 9 \equiv 2 \pmod{11},$$

$$13 \times 13^3 + 3 \times 13 \equiv 2 \times 2^3 + 3 \times 2 \equiv 7 \pmod{11}$$

This was expected since $[2] = [13]$

# Polynomials Mod $m$

## Example

The polynomial $x^2 - 2x - 1$ has no integer roots (it has the real roots $1 - \sqrt{2}$ and $1 + \sqrt{2}$). However, evaluating at [4] and [5] mod 7 yields [0], so we consider [4] and [5] to be its roots mod 7.

## Example

The equation $x^2 - 1$ has roots $\pm 1$ in the integers and thus has roots $[1], [-1]$ mod $m$ for any $m$. However, it has the additional roots [8] and [17] mod 21 (check for yourself!). No quadratic equation over the real numbers has more than two real roots - modular arithmetic changes the rules of polynomial factorization!

# Polynomials Mod $m$

**Exercise**

*Find the four roots of the polynomial* $x^4 - 1$ *mod* $5$.

**Exercise**

*Find a modulus* $m$ *such that* $x^2 + 1$ *has two roots. You can think of these roots as being square roots of* $[-1]$.

# Primality and Polynomials Mod $m$

Let $k$ be the number of distinct prime factors of $m$. It is a fact that the number of roots mod $m$ of $x^2 - 1$ is $2^k$. In particular, if $m$ is prime, then $k = 1$ and the only roots are $\pm 1$. We exploit this to obtain a new primality test.

# Miller-Rabin Test

- Express $m - 1 = 2^s t$, where $t$ is odd.
- Choose an integer $a$ (usually between 2 and $n - 1$).
- If $a^t \equiv 1 \pmod{m}$, $m$ is "probably prime"; we are finished.
- For each $r$ between 1 and $s$ inclusive, check whether $a^{2^r t} \equiv 1 \pmod{m}$.
- If no such $r$ exists, then in particular $a^{m-1} \equiv a^{2^s t} \not\equiv 1 \pmod{m}$ and thus $m$ is composite by Fermat's Little Theorem; we are finished.
- Else, for the first such $r$, check whether $a^{2^{r-1} t} \equiv -1 \pmod{m}$.
- If not, then $a^{2^{r-1} t}$ is an additional root to $x^2 - 1 \bmod m$; thus $m$ is composite and we are finished.
- Else $m$ is "probably prime"; we are finished.

# Miller-Rabin Test

## Example

Let's run the Miller-Rabin test on the Carmichael number $m = 561$ with $a = 2$. Write $m - 1 = 560 = 2^4 \times 35$. We calculate as follows:

- $2^{35} \equiv 263 \pmod{561}$
- $2^{70} \equiv 166 \pmod{561}$
- $2^{140} \equiv 67 \pmod{561}$
- $2^{280} \equiv 1 \pmod{561}$

But this means that $[2^{140}]$ is a root of $x^2 - 1$ which is neither $[-1]$ nor $[1]$. Therefore 561 is proven composite, as opposed to the Fermat test with $a = 2$ which would have suggested "probably prime".

# Miller-Rabin Test

Like the Fermat test, there are Miller-Rabin pseudoprimes to any base $a$ (composite $m$ for which the Miller-Rabin test with $a$ returns "probably prime"). But unlike the Carmichael numbers, at most $1/4$ (and usually significantly fewer) of the integer $a$ between 2 and $m-1$ inclusive will fail to identify composite $m$. This gives rise to a probabilistic method of identifying primes.

## Example

Fix $m$ and suppose that we choose 10 different bases $a$ between 2 and $m-1$ at random. Suppose also that running Miller-Rabin on all 10 bases returns "probably prime". Then we conclude that there is less than a $(1/4)^10 \approx 10^{-6}$ chance that $m$ is composite.

## Exercise

*How many bases must we choose to theoretically have a 99% chance that $m$ is prime?*

# Being Absolutely Sure

How can we use the Miller-Rabin test to *prove* that a number is prime with no margin of error? By sophisticated methods, Heath-Brown has shown that for all composite $m$ past some uncomputed point $m_0$, there is at least one Miller-Rabin witness for $m$ less than $\sqrt[10]{m}$. Assuming the truth of the Extended Riemann Hypothesis (a famous open conjecture), it was shown by Bach that there is at least one Miller-Rabin witness for $m$ less than $2(\ln(m))^2$. Both these bounds are far smaller than the trial factoring bound $\sqrt{m}$.