UCLA Math Circle

James Toche (and family)

2 August 2020
(Last revision: August 4, 2020)

Abstract

Notes on modular arithmetic from the UCLA Math Circle Intermediate-2 for Summer Session 2020, August 2nd.

1.2

If $a \equiv b \pmod{m}$, then $(a+m) \equiv b \pmod{m}$

Let $\pmod{m}$ denote "modulo m". The first statement is equivalent to:

$$a \equiv b \pmod{m} \iff \exists k \in \mathbb{N} : a = km + b$$

where b is the remainder of the division of a by the modulus m.

The second statement is equivalent to:

$$(a+m) \equiv b \pmod{m} \iff \exists l \in \mathbb{N} : a + m = lm + b$$

Proof: $\exists k \in \mathbb{N}$:

$$\begin{aligned} a &= km + b \\ a + m &= km + b + m \\ a + m &= (k+1)m + b \end{aligned}$$

We set $l = k + 1$, where $l \in \mathbb{N}$ since k and 1 are in $\mathbb{N}$. $\square$

2.1

If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

The starting point is:

$$\begin{aligned} \exists k \in \mathbb{N}: \quad a = km + b \\ \exists l \in \mathbb{N}: \quad b = lm + c \end{aligned}$$

for a, b, c in $\mathbb{N}$. By simple substitution,

$$\begin{aligned} a &= km + b \\ &= km + lm + c \\ &= (k + l)m + c \end{aligned}$$

where $(k + l) \in \mathbb{N}$ since $k \in \mathbb{N}$ and $l \in \mathbb{N}$. Thus, a leaves a remainder of c after division by m. The last line is equivalent to

$$a \equiv c \pmod{m} \qquad \square$$

2.2

If $\boldsymbol{a \equiv b \pmod{m}}$ and $\boldsymbol{c \equiv d \pmod{m}}$, then $\boldsymbol{(a+c) \equiv (b+d) \pmod{m}}$ and $\boldsymbol{ac \equiv bd \pmod{m}}$.

The starting point is:

$$\begin{aligned} \exists k \in \mathbb{N}: &\qquad a = km + b \\ \exists l \in \mathbb{N}: &\qquad c = lm + d \end{aligned}$$

for a, b, c, d in $\mathbb{N}$.

There are two statements to be proved. Start with $(a + c)$. By simple addition,

$$\begin{aligned} a + c &= (km + b) + (lm + d) \\ &= (k + l)m + (b + d) \end{aligned}$$

where $(k + l) \in \mathbb{N}$ since k, l are in $\mathbb{N}$. The last line is equivalent to

$$a + c \equiv b + d \pmod{m} \qquad \square$$

Turn to (ac). By multiplication,

$$\begin{aligned} ac &= (km + b) \times (lm + d) \\ &= (klm + kd + bl)m + bd \end{aligned}$$

where $(klm + kd + bl) \in \mathbb{N}$ since k, l, b, d, m are all in $\mathbb{N}$ and so are their sums and products.

$$ac \equiv bd \pmod{m} \qquad \square$$

2.3

If $a \equiv b \pmod{m}$ then $a^k \equiv b^k \pmod{m}$ for all $k \geq 1$.

Suppose the following is true for $k = 1$ and some $k > 1$:

$$\begin{aligned} P(1): &\qquad a = lm + b \quad \text{for some } l \in \mathbb{N} \\ P(k): &\qquad a^k = qm + b^k \quad \text{for some } q \in \mathbb{N} \end{aligned}$$

for a, b, m, k in $\mathbb{N}$. The factor q is "unimportant" and will typically vary with k. We also assume that $b < m$, that is the remainder has been reduced to its "standard representation" for modulus m. However, the remainder b^k could be greater than m (only for $b = 0$ or $b = 1$ is $b^k < m$ guaranteed).

Base Case:

$$\begin{aligned} P(2): \qquad a^2 &= (lm + b)^2 \\ &= (lm)^2 + 2lmb + b^2 \\ &= m(l^2 m + 2lb) + b^2 \\ &\equiv b^2 \pmod{m} \qquad \checkmark \end{aligned}$$

This immediately suggests a direct proof based on the binomial expansion formula.

Direct Proof:

The binomial expansion formula for any a, b is:

$$\begin{aligned} (a+b)^n &= a^n + na^{n-1}b + \ldots + \frac{n!}{k!(n-k)!} a^{n-k} b^k + \ldots + nab^{n-1} + b^n \\ &= \sum_{k=0}^{k=n} \binom{n}{k} a^k b^{n-k} \end{aligned}$$

where $\sum$ denotes the sum over the index k running from 0 to n, and $\binom{n}{k}$ the binomial coefficient:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

The first few values of the binomial coefficient may be arranged to form the well-known Pascal triangle:

$$\begin{array}{c|ccccccccc} n=0 & & & & & 1 & & & & \\ n=1 & & & & 1 & & 1 & & & \\ n=2 & & & 1 & & 2 & & 1 & & \\ n=3 & & 1 & & 3 & & 3 & & 1 & \\ n=4 & 1 & & 4 & & 6 & & 4 & & 1 \end{array}$$

or explicitly:

$$\begin{array}{c|ccccccccc} n=0 & & & & & \binom{0}{0}=1 & & & & \\ n=1 & & & & \binom{1}{0}=1 & & \binom{1}{1}=1 & & & \\ n=2 & & & \binom{2}{0}=1 & & \binom{2}{1}=2 & & \binom{2}{2}=1 & & \\ n=3 & & \binom{3}{0}=1 & & \binom{3}{1}=3 & & \binom{3}{2}=3 & & \binom{3}{3}=1 & \\ n=4 & \binom{4}{0}=1 & & \binom{4}{1}=4 & & \binom{4}{2}=6 & & \binom{4}{3}=4 & & \binom{4}{4}=1 \end{array}$$

Apply the binomial expansion formula to $(lm+b)^k$:

$$\begin{aligned}
a^k &= (qm+b)^k \\
&= (qm)^k + k(qm)^{k-1}b + \ldots + k(qm)b^{k-1} + b^k \\
&= m \times \underbrace{(\ldots)}_{\in \mathbb{N}} + b^k \quad \text{if } k > 0 \\
&\equiv b^k \pmod{m}
\end{aligned}$$

The details of what goes into $(\ldots)$ are unimportant, as long as it is in $\mathbb{N}$ — what matters is that the modulus m may be factored, which is true if $k > 0$. Now go back to the proof by induction.

Induction Step:

Show that the left-hand side of $P(k+1)$ is congruent to b^{k+1} modulo m:

$$\begin{aligned}
\texttt{lhs} &= (qm+b)^{k+1} \\
&= \underbrace{(qm+b)^k}\ (qm+b) \\
&= (mp+b^k)\ (qm+b) \\
&= mpqm + mpb + b^k qm + b^k b \\
&= m(\underbrace{pqm + pb + b^k q}_{\in \mathbb{N}}) + b^{k+1} \\
&\equiv b^{k+1} \pmod{m} \\
&= \texttt{rhs} \qquad \square
\end{aligned}$$

3

If $3 \nmid x$ and $3 \nmid y$, then $3|(x^2 - y^2)$.

$3 \nmid x$ reads as "3 does not divide x." In words, "if 3 divides neither x nor y, it must divide the difference of their squares $x^2 - y^2$."

The "does-not-divide" property may be stated as:

$$\begin{aligned} x &= 3k + r, \quad r \neq 0 \\ y &= 3l + s, \quad s \neq 0 \end{aligned}$$

In words, "3 is not a factor of x if the remainder is non-zero." Same goes for y. Combining these two properties yields:

$$\begin{aligned} x^2 - y^2 &= (3k + r)^2 - (3l + s)^2 \\ &= (3k)^2 - (3l)^2 + 2(3k)r - 2(ls) + r^2 - s^2 \\ &= 3\ (\underbrace{3k^2 - 3l^2 + 2kr - 2ls}_{\in \mathbb{N}})\ + r^2 - s^2 \end{aligned}$$

If $3|(x^2 - y^2)$, we must have $r^2 - s^2 \equiv 0 \pmod 3$. The only possible values of r and s are 1 and 2. So let's see: if $r = s$, then $r^2 - s^2 = 0$, otherwise let $r = 2$ and $s = 1$:

$$\begin{aligned} & r^2 - s^2 = 2^2 - 1^2 = 4 - 1 = 3 \\ \text{or} \quad & r^2 - s^2 = 1^2 - 2^2 = 1 - 4 = -3 \end{aligned}$$

In both cases, these are multiples of 3. And so it follows that

$$x^2 - y^2 \equiv 0 \pmod 3 \qquad \square$$

4

Prove that for all integers n, either $n^2 \equiv 0 \pmod 4$ or $n^2 \equiv 1 \pmod 4$.

It is convenient to split the proof between even and odd integers. For any $n \in \mathbb{N}$ (even or odd), we can write the integer as a sum of a multiple of 4 and a remainder r:

$$n = 4k + r \quad \text{for some } k, r \text{ in } \mathbb{N}$$

Even Integers:

All even integers may be written as $2n$ for some $n \in \mathbb{N}$. Thus, the square of an even integer may be written:

$$\begin{aligned}
(2n)^2 &= (2(4k+r))^2 \\
&= 4 \times \underbrace{(4k+r)^2}_{\in \mathbb{N}} \quad + 0 \\
&\equiv 0 \pmod 4 \qquad \square
\end{aligned}$$

In words, this statement is pretty obvious: "The square of an even integer is a multiple of 4." Figure 1 illustrates modular arithmetic with a number wheel: Numbers stacked within the same slice have the same remainder modulo 4. The squares of even integers all belong to the same quarter-slice of the wheel: $0, 4, 16, 36,$ *etc.*. The same wheel also shows that the squares of odd numbers stack up within the same slice: $1, 9, 25,$ *etc.*.

Odd Integers:

All odd integers may be written as $2n + 1$ for some $n \in \mathbb{N}$. So the square of an odd integer:

$$\begin{aligned}
(2n+1)^2 &= (2(4k+r)+1)^2 \\
&= (2(4k+r))^2 + 2 \cdot 2(4k+r) \cdot 1 + 1^2 \\
&= 4 \times \underbrace{((4k+r)^2 + (4k+r))}_{\in \mathbb{N}} \quad + \ 1 \\
&\equiv 1 \pmod 4 \qquad \square
\end{aligned}$$

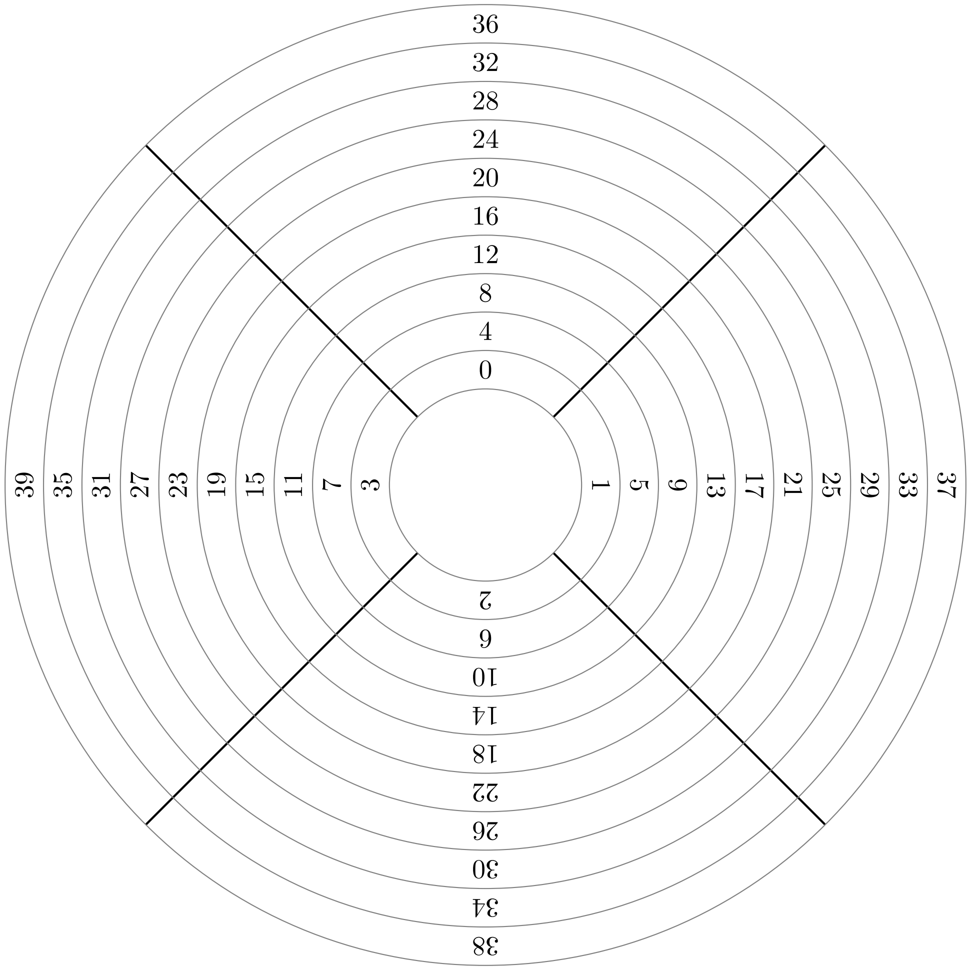

Figure 1: **Modular Arithmetic: Number Wheel Modulo** 4**.**