HISTORY OF MATHEMATICS
MATHEMATICAL TOPIC VII
MODULAR ARITHMETIC

PAUL L. BAILEY

ABSTRACT. Congruence relations were formalized by Gauss at the beginning of the nineteenth century; however, important components of the theory were realized by the ancient Greeks, Arabs, and Chinese. We investigate this, with an eye towards understanding the Chinese Remainder Theorem.

1. Review of Integer Properties

Fact 1. Division Algorithm for Integers
Let $m, n \in \mathbb{Z}$. There exist unique integers $q, r \in \mathbb{Z}$ such that

$$n = qm + r \qquad \text{and} \qquad 0 \leq r < m.$$

Definition 1. Let $m, n \in \mathbb{Z}$. We say that m *divides* n, and write $m \mid n$, if there exists an integer k such that $n = km$.

Definition 2. Let $m, n \in \mathbb{Z}$. A *greatest common divisor* of m and n, denoted $\gcd(m, n)$, is a positive integer d such that

(1) $d \mid m$ and $d \mid n$;
(2) If $e \mid m$ and $e \mid n$, then $e \mid d$.

Fact 2. Euclidean Algorithm for Integers
Let $m, n \in \mathbb{Z}$. Then there exists a unique $d \in \mathbb{Z}$ such that $d = \gcd(m, n)$, and there exist integers $x, y \in \mathbb{Z}$ such that

$$xm + yn = d.$$

Definition 3. An integer $p \geq 2$, is called *prime* if

$$a \mid p \Rightarrow a = 1 \text{ or } a = p, \quad \text{where } a \in \mathbb{N}.$$

An integer $n \geq 2$ is called *composite* if it is not prime.

Fact 3. Fundamental Theorem of Arithmetic
Let $n \in \mathbb{Z}$, $n \geq 2$. Then there exist unique prime numbers $p_1 < \cdots < p_r$ and positive integers $a_1, \dots, a_r$ such that

$$n = \prod_{i=1}^{r} p_i^{a_i}.$$

Date: October 27, 2006.

2. Congruence Modulo n

Proposition 1. *Let $n \in \mathbb{Z}$ with $n \geq 2$, and let $a, b, c \in \mathbb{Z}$. Then*

- **(a)** $a \equiv a \pmod{n}$ *(Reflexivity);*
- **(b)** *if* $a \equiv b \pmod{n}$*, then* $b \equiv a \pmod{n}$ *(Symmetry);*
- **(c)** *if* $a \equiv b \pmod{n}$ *and* $b \equiv c \pmod{n}$*, then* $a \equiv c \pmod{n}$ *(Transitivity).*

Proof.
(*Reflexivity*) Note that $0 \cdot n = 0 = a - a$; thus $n \mid (a - a)$, so $a \equiv a$. Therefore $\equiv$ is reflexive.
(*Symmetry*) Let $a, b \in \mathbb{Z}$. Suppose that $a \equiv b$; then $n \mid (a - b)$. Then there exists $k \in \mathbb{Z}$ such that $nk = a - b$. Then $n(-k) = b - a$, so $n \mid (b - a)$. Thus $b \equiv a$. Similarly, $b \equiv a \Rightarrow a \equiv b$. Therefore $\equiv$ is symmetric.
(*Transitivity*) Let $a, b, c \in \mathbb{Z}$, and suppose that $a \equiv b$ and $b \equiv c$. Then $nk = a - b$ and $nl = b - c$ for some $k, l \in \mathbb{Z}$. Then $a - c = nk - nl = n(k - l)$, so $n \mid (a - c)$. Thus $a \equiv c$. Therefore $\equiv$ is transitive. □

Proposition 2. *Let $n \in \mathbb{Z}$ with $n \geq 2$. Let $a, b \in \mathbb{Z}$. Then* $a \equiv b \pmod{n}$ *if and only if a and b have the same remainder upon division by n.*

Proof. By the division algorithm, there exist unique integer q_1, q_2, r_1, r_2 such that

$$a = nq_1 + r_1 \quad \text{with } 0 \leq r_1 \leq n$$

and

$$b = nq_2 + r_2 \quad \text{with } 0 \leq r_2 \leq n.$$

Thus $a - b = n(q_1 - q_1) + (r_1 - r_2)$.

If $a \equiv b \pmod{n}$, then $n \mid (a - b)$, so $a - b = kn$ for some $k \in \mathbb{Z}$. Thus $kn = n(q_1 - q_2) + (r_1 - r_2)$, so $r_1 - r_2 = n(k - q_1 + q_2)$; that is, $r_1 - r_2$ is a multiple of n. But subtracting the inequalities bounding the remainders shows that $-n < r_1 - r_2 < n$, and the only multiple of n in this range is zero. So $r_1 - r_2 = 0$, whence $r_1 = r_2$.

On the other hand, if $r_1 = r_2$, then we have $a - b = n(q_1 - q_2)$, so $a - b$ is divisible by n, and $a \equiv b \pmod{n}$. □

Proposition 3. *Let $n \in \mathbb{Z}$ with $n \geq 2$. Let $a, b, c, d \in \mathbb{Z}$ with $a \equiv c$ and $b \equiv d$. Then*

- **(a)** $a + b \equiv c + d \pmod{n}$*;*
- **(b)** $ab \equiv cd \pmod{n}$.

Proof. All equivalences will be taken modulo n. Since $a \equiv c$ and $b \equiv d$, there exist $p, q \in \mathbb{Z}$ such that $a - c = pn$ and $b - d = qn$.

Now $a + b = c + pn + d + qn = (c + d) + n(p + q)$, so $(a + b) - (c + d) = n(p + q)$, whence $a + b \equiv c + d$.

Similarly, $ab = (c + pn)(d + qn) = cd + cqn + dpn + pqn^2 = cd + n(cq + dp + pqn)$, whence $ab - cd = n(cq + dp + pqn)$, so $ab - cd$ is divisible by n. Thus $ab \equiv cd$. □

3. Casting Out n's

The process of *casting out n's* involves subtracting n from a number until one arrives at a number less than n. Clearly, this number is the remainder upon division by n, so it is related to modular arithmetic.

The method of casting out n's, together with decimal notation, led Arabs of 1500 years ago to discover certain divisibility criteria. We demonstrate this in modern notation.

Fix $n \in \mathbb{Z}$ with $n \geq 0$. For $a \in \mathbb{Z}$, let $\overline{a}$ denote the remainder when a is divide by n. The last proposition states that $\overline{a+b} \equiv \overline{a} + \overline{b}$ and $\overline{ab} \equiv \overline{a}\overline{b}$, modulo n.

If $d_0, d_1, \ldots, d_r$ are the digits of $a \in \mathbb{N}$, then

$$a = \sum_{i=0}^{r} d_i 10^i.$$

The idea of casting out n's revolves around the fact that

$$a \equiv \sum_{i=0}^{r} \overline{d_i}\,\overline{10}^i \pmod{n}.$$

Proposition 4. Casting Out 3's and 9's
Let $a \in \mathbb{Z}$ be a positive integer with decimal expansion

$$a = \sum_{i=0}^{k} d_i 10^i,$$

where $0 \leq d_i \leq 9$ for $i = 0, \ldots, k$. Set

$$s = \sum_{i=0}^{k} d_i$$

Let $n = 3$ or $n = 9$. Then a is divisible by n if and only if s is divisible by n.

Proof. Let $n = 3$ or $n = 9$ and consider equivalence modulo n. Note that $10 \equiv 1 \pmod{n}$ for $n = 3$ or $n = 9$. Then we have

$$\begin{aligned} a &= \overline{\sum_{i=0}^{k} d_i 10^i} \\ &\equiv \sum_{i=0}^{k} d_i \overline{10}^i \\ &\equiv \sum_{i=0}^{k} d_i \quad \text{because} \quad \overline{10} = 1 \\ &= s. \end{aligned}$$

So a and s have the same remainder upon division by n, and in particular a is divisible by n if and only if s is divisible by n. □

Proposition 5. Casting Out 11's
Let $a \in \mathbb{Z}$ be a positive integer with decimal expansion

$$a = \sum_{i=0}^{k} d_i 10^i,$$

where $0 \leq d_i \leq 9$ for $i = 0, \ldots, k$. Set

$$s = \sum_{i=0}^{k} (-1)^i d_i$$

Let $n = 11$. Then a is divisible by n if and only if s is divisible by n.

Proof. Let $n = 11$. In this case, $10 \equiv -1 \pmod{n}$. We have

$$\begin{aligned} a &= \sum_{i=0}^{k} d_i 10^i \\ &\equiv \sum_{i=0}^{k} d_i \overline{10}^i \\ &\equiv \sum_{i=0}^{k} d_i \overline{-1}^i \\ &\equiv \sum_{i=0}^{k} (-1)^i d_i \\ &= s. \end{aligned}$$

Thus a is divisible by n if and only if s is divisible by n. □

4. Chinese Remainder Theorem

Proposition 6. *Let* $a, b, m, n \in \mathbb{Z}$ *such that* $\gcd(m, n) = 1$.
Then there exists $c \in \mathbb{Z}$ *such that*

- $c \equiv a \mod m$;
- $c \equiv b \mod n$.

Proof. There exist $x, y \in \mathbb{Z}$ such that $mx + ny = 1$. Let $c = mxb + nya$. Then

$$c - a = mxb + nya - a = mxb + (ny - 1)a = mxb - mxa,$$

so m divides $c - a$; thus $c \equiv a \mod m$. Also

$$c - b = mxb + nya - b = (mx - 1)b + nya = -nyb + nya,$$

so n divides $c - b$; thus $c \equiv b \mod n$. □

Example 1. Let $m = 104$, $n = 231$, $a = 11$, and $b = 23$. Find $c \in \mathbb{Z}$ with $0 \leq c < mn$ such that $c \equiv a \pmod{m}$ and $c \equiv b \pmod{n}$.

Solution. First we use the Euclidean algorithm to write $mx + yn = d$. We have

$$\begin{aligned} 231 &= 104 \cdot 2 + 23 \\ 104 &= 23 \cdot 4 + 12 \\ 23 &= 12 \cdot 1 + 11 \\ 12 &= 11 \cdot 1 + 1 \\ 11 &= 1 * 11 + 0 \end{aligned}$$

Thus

$$\begin{aligned} 1 &= (-1)11 + 12 \\ &= (2)12 + (-1)23 \\ &= (-9)23 + (2)104 \\ &= (20)104 + (-9)231 \end{aligned}$$

That is, $x = 20$, $y = -9$, and $d = 1$,

Now set

$$c = mxb + nya \pmod{24024} = 24971 \pmod{24024} = 947.$$

□

Department of Mathematics and CSci, Southern Arkansas University
E-mail address: plbailey@saumag.edu