Modular Arithmetic

Because $0, 1, 2, \ldots, n-1$ gives a complete residue system (mod n), it follows that any combination of sums, differences and products of these numbers will be congruent (mod n) to a unique number in this residue system. This leads to the concept of modular arithmetic.

For example, consider the set $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ where $0, 1, 2, 3, 4, 5$ is a complete residue system (mod 6). Notice that $3 + 5 \equiv 2 \pmod 6$ and $3 + 3 \equiv 0 \pmod 6$. In addition, we see that $3 \cdot 5 \equiv 3 \pmod 6$ and $3 \cdot 3 \equiv 3 \pmod 6$. So, we can perform arithmetic on the set $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$. Below is an addition table and a multiplication table for modular arithmetic on the set $\mathbb{Z}_6$.

$a+^b$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$a + b (\text{mod } 6)$

$a\cdot^b$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

$a \cdot b (\text{mod } 6)$

Table 3.1: Modular Arithmetic (mod 6)

For another example, consider $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ where $0, 1, 2, 3, 4$ is a complete residue system (mod 5). Notice that $3 + 2 \equiv 0 \pmod 5$ and $3 + 3 \equiv 1 \pmod 5$. In addition, we see that $3 \cdot 4 \equiv 2 \pmod 5$ and $3 \cdot 3 \equiv 4 \pmod 5$. Below is an addition table and a multiplication table for modular arithmetic on the set $\mathbb{Z}_5$.

$a+^b$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$a + b (\text{mod } 5)$

$a\cdot^b$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$a \cdot b (\text{mod } 5)$

Table 3.2: Modular Arithmetic (mod 5)

Problem 10. Show that every perfect square is congruent to 0, 1 or 4 (mod 5).

Solution. Let n be a perfect square. So $n = k^2$ for some integer k. Theorem 3.2.8 asserts that either $k \equiv 0 \pmod 5$, $k \equiv 1 \pmod 5$, $k \equiv 2 \pmod 5$, $k \equiv 3 \pmod 5$ or $k \equiv 4 \pmod 5$. Thus, either $k^2 \equiv 0^2 \pmod 5$, $k^2 \equiv 1^2 \pmod 5$, $k^2 \equiv 2^2 \pmod 5$, $k^2 \equiv 3^2 \pmod 5$ or $k^2 \equiv 4^2 \pmod 5$. Since $9 \equiv 4 \pmod 5$ and $16 \equiv 1 \pmod 5$, we conclude that either $k^2 \equiv 0 \pmod 5$, $k^2 \equiv 1 \pmod 5$, or $k^2 \equiv 4 \pmod 5$.

Polynomials with Integer Coefficients

Definition 3.2.11. A function $f(x)$ of the form $f(x) = a_k x^k + a_{k-1}x^{k-1} + \cdots + a_1 x + a_0$ were $a_k, a_{k-1}, \ldots, a_1, a_0$ are all integers is called a **polynomial with integer coefficients**.

Note that if $f(x)$ is a polynomial with integer coefficients, then for any integer a, the value $f(a)$ will also be integer.

Example 11. The functions $f(x) = 3x^4 - 2x^2 + 5x + 4$ and $g(x) = 5x^3 - 9x^2 - x + 10$ are polynomials with integer coefficients. Notice that whenever a is an integer then $f(a)$ and $g(a)$ will also be integers. For example, $f(2) = 54$, $f(-2) = 34$, $g(-5) = -835$ and $g(5) = 405$.

Theorem 3.2.12 (Substitution Theorem)**.** Let $f(x)$ be a polynomial with integer coefficients. If $a \equiv b \pmod{n}$, then $f(a) \equiv f(b) \pmod{n}$.

Proof. Let $f(x) = a_k x^k + a_{k-1}x^{k-1} + \cdots + a_1 x + a_0$ where $a_k, a_{k-1}, \ldots, a_1, a_0$ are all integers. Assume that $a \equiv b \pmod{n}$. Then, by Theorems 3.2.2 and 3.2.5, we see that

$$(a_k a^k + a_{k-1}a^{k-1} + \cdots + a_1 a + a_0) \equiv (a_k b^k + a_{k-1}b^{k-1} + \cdots + a_1 b + a_0) \pmod{n}.$$

Therefore, $f(a) \equiv f(b) \pmod{n}$. □

Applications of Theorem 3.2.12

Is there is a simple method that will always produce prime numbers? More specifically:

> Is there a polynomial $f(x)$, of degree 1 or higher, with integer coefficients such that $f(m)$ is a prime number for *every* integer m?

Theorem 3.2.13. Let $f(x)$ be a polynomial, of degree 1 or higher, with integer coefficients. Then there exist an integer m such that $f(m)$ is not a prime number.

Proof. Let $f(x)$ be a polynomial, of degree 1 or higher, with integer coefficients. Suppose, for a contradiction, that $f(m)$ is a prime number for every integer m. Let $f(x)$ have the form $f(x) = a_k x^k + a_{k-1}x^{k-1} + \cdots + a_1 x + a_0$ were $a_k, a_{k-1}, \ldots, a_1, a_0$ are all integers. Since $f(m)$ is always a prime number, it follows that $a_k > 0$. Furthermore, since $a_k > 0$, it follows that $f(x)$ gets larger and larger as x gets larger and larger. Thus, there must be an integer a such that $f(a) > 1$. Let $n = f(a)$. Again, because $f(x)$ gets larger and larger as x gets larger and larger, there is a natural number j such that $f(a + jn) > n$. So, from our assumption, we must have that $f(a + jn)$ is a prime. Now, note that $(a + jn) \equiv a \pmod{n}$. Theorem 3.2.12 asserts that $f(a + jn) \equiv f(a) \pmod{n}$. Since $f(a) = n$, we conclude that $f(a + jn) \equiv f(a) \equiv n \equiv 0 \pmod{n}$. Hence, $f(a + jn) \equiv 0 \pmod{n}$ and thus, $n \mid f(a + jn)$ where $1 < n < f(a + jn)$. Therefore, $f(a + jn)$ is not a prime number. This contradiction shows that there must exist an integer m where $f(m)$ is not a prime. □

We now recall that we express our integers $n > 0$ using decimal notation. For example, the natural number $6,235$ is in decimal notation. So,

$$6,235 = 6 \cdot 10^3 + 2 \cdot 10^2 + 3 \cdot 10 + 5.$$

So every integer $n > 0$ can be expressed in the form

$$n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0 \tag{3.8}$$

where $a_k, a_{k-1}, \ldots, a_1, a_0$ are the digits of n from left to right. So, a_k is the left most digit and a_0 is the rightmost digit. Each digit a_i is between 0 and 9. Now, let $f(x)$ be the polynomial (with integer coefficients) defined by

$$f(x) = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_1 x + a_0.$$

Hence,

$$f(10) = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0 = n$$

and

$$f(1) = a_k 1^k + a_{k-1} 1^{k-1} + \cdots + a_1 1 + a_0 = a_k + a_{k-1} + \cdots + a_1 + a_0.$$

Clearly, $10 \equiv 1 \pmod 9$. Thus, Theorem 3.2.12 implies that $f(10) \equiv f(1) \pmod 9$. We conclude that

$$n \equiv (a_k + a_{k-1} + \cdots + a_1 + a_0) \pmod 9. \tag{3.9}$$

Thus, any natural number is congruent to the sum of its digits (mod 9).

Theorem 3.2.14. Let n be a natural number. Then n is evenly divisible by 9 if and only if the sum of its digits is evenly divisible by 9.

Proof. Let $s = a_k + a_{k-1} + \cdots + a_1 + a_0$ be the sum of the digits in the decimal expression of n. By (3.9) we have that $(\star)$ $n \equiv s \pmod 9$. If $9 \mid n$, then $n \equiv 0 \pmod 9$. Thus, $(\star)$ implies that $s \equiv 0 \pmod 9$ and therefore, $9 \mid s$. Conversely, if $9 \mid s$, then $s \equiv 0 \pmod 9$. Thus, $(\star)$ implies that $n \equiv 0 \pmod 9$ and therefore, $9 \mid n$. □

Example 12. Decide whether or not the following natural numbers n are divisible by 9.

1. $n = 111,105$
2. $n = 518,933$
3. $n = 51,893,618,931$.

Problem 13. Show that

$$31 \mid (59 \cdot 63^{23} + 6 \cdot 63^{45} - 3).$$

Hint: $63 \equiv \underline{\ ?\ } \pmod{31}$

Solution. We shall show that $(59 \cdot 63^{23} + 6 \cdot 63^{45} - 3) \equiv 0 \pmod{31}$. Since $63 \equiv 1 \pmod{31}$, we see that $63^{23} \equiv 1^{23} \pmod{31}$ and $63^{45} \equiv 1^{45} \pmod{31}$. Thus, we have the following:

$$\begin{aligned} (59 \cdot 63^{23} + 6 \cdot 63^{45} - 3) &\equiv (59 \cdot 1^{23} + 6 \cdot 1^{45} - 3) \pmod{31} \\ &\equiv (59 + 6 - 3) \pmod{31} \\ &\equiv 62 \pmod{31} \\ &\equiv 0 \pmod{31}. \end{aligned}$$

Therefore, $(59 \cdot 63^{23} + 6 \cdot 63^{45} - 3) \equiv 0 \pmod{31}$ and thus, $31 \mid (59 \cdot 63^{23} + 6 \cdot 63^{45} - 3)$.

Problem 14. Show that

$$31 \,|\, (5(64)^3 + 6(34)^2 - 1).$$

Hint: $64 \equiv \underline{\ ?\ } \pmod{31}$ and $34 \equiv \underline{\ ?\ } \pmod{31}$

Problem 15. Let m and n be arbitrary positive integers. Show that

$$19 \,|\, (13(20)^m + 56(39)^n + 7).$$

Problem 16. Let $n = a_4 10^4 + a_3 10^3 + a_2 10^2 + a_1 10 + a_0$. Show that

$$n \equiv (a_4 - a_3 + a_2 - a_1 + a_0) \pmod{11}.$$

Hint: $10 \equiv -1 \pmod{11}$.

Exercises 3.2

Do problems #13, 15, 16, 23, 29, 33 on pages 64-66 of text.

Exercise Notes.

- Problem 13: $4,926,834,923 = 4,926,834,920 + 3$. Equation (3.8) (above) implies that $4 \,|\, 4,926,834,920$. Now, show that $4,926,834,923 \equiv 3 \pmod{4}$.
- Problem 15: Use the fact that $5^2 \equiv 2^3 \pmod{17}$.
- Problem 16: Use a similar idea as in the the above hint for Problem 15.
- Problem 29: There are an infinite number of integers n with $n \equiv 1 \pmod{43}$.
- Problem 33: Since $n^2 + 2$ and $n^2 - 2$ are both prime, it follows that $n^2 + 2 > 3$ and $n^2 + 2$ not divisible by 3. To prove that $3 \,|\, n$, show that $n \equiv 0 \pmod{3}$ by establishing that n is not congruent to 1 or 2 (mod 3).