3. Theorems

Theorem: Given any integer $b > 1$, any integer may be written uniquely in base b place-value notation.

Proof: repeated applications of the division algorithm.

Theorem 4.4: Let $P(x) = \sum_{k=0}^{m} c_k x^k$ be a polynomial function of x with integral coefficients c_k. If $a \equiv b(\text{mod n})$, then $P(a) \equiv P(b)(\text{mod n})$.

Proof:

$$a \equiv b(\text{mod n}) \Longrightarrow a^k \equiv b^k(\text{mod n})$$

Therefore,

$$c_k a^k \equiv c_k b^k(\text{mod n})$$

and the sums of all the coefficients are equal as well, i.e. $P(a) \equiv P(b)(\text{mod n})$.

Corollary: If a is a solution of the **congruence** $P(x) \equiv 0(\text{mod n})$, and $a \equiv b(\text{mod n})$, then b is also a solution.

Theorem 4.5/4.6: Let $(a_m\, a_{m-1} \cdots a_2\, a_1\, a_0)_{10}$

$$N = a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_2 10^2 + a_1 10 + a_0 = P(10)$$

be the decimal expansion of positive integer N, $0 \leq a_k \quad 10$, and let $S = a_0 + a_1 + \ldots + a_m$. Then

So $P(x) = a_m x^m + \ldots + a_2 x^2 + a_1 x + a_0$.

- $9|N \iff 9|S$.

$3621 = 3 \cdot 10^3 + 6 \cdot 10^2 + 2 \cdot 10^1 + 1 \cdot 10^0$

N is divisible by 9 $\Rightarrow$ $N \equiv 0 \pmod 9$

$10 \equiv 1 \pmod 9 \Rightarrow P(10) \equiv P(1) \pmod 9$

$P(1) = a_m \cdot 1^m + a_{m-1} \cdot 1^{m-1} + \ldots + a_2 1^2 + a_1 \cdot 1^1 + a_0$

$= a_m + a_{m-1} + \ldots + a_2 + a_1 + a_0 = S$

$\therefore N \equiv S \pmod 9$

So if $N \equiv 0 \pmod 9$ (i.e. $9 | N$) then $S \equiv 0 \pmod 9$ (i.e. $9 | S$), & vice versa.

- Let $T = a_0 - a_1 + a_2 - \ldots + (-1)^m a_m$. Then $11|N \iff 11|T$.

$10 \equiv -1 \pmod{11}$; hence $P(10) \equiv P(-1) \pmod{11}$

$$\therefore\ N \equiv \underbrace{a_m(-1)^m + a_{m-1}(-1)^{m-1} + \ldots + a_2(-1)^2 + a_1(-1)^1}_{T} + a_0 \pmod{11}$$

So if $11 \backslash N$ then $11 \backslash T$ & vice versa.

4. Properties/Tricks/Hints/Etc.

Often "the trick" to solving the problems involves

- figuring out which n in "modulo n" we need, or
- figuring out how to rewrite things modulo n so that good things happen.

#3 p73

Divisible by 9 or 11?

	9	11
176,521,221	✓	×
149,235,678	✓	×

27	-3
45	9

#1a units digit of a^2 is 0, 1, 4, 5, 6, 9

Want $a^2 \pmod{10}$

$a \equiv r \pmod{10}$ where $r \in \{0, 1, \ldots, 9\}$

$a^2 \equiv r^2 \pmod{10}$

Cases

$$
\begin{array}{ll}
r=0 & r^2 \equiv 0 \pmod{10} \\
1 & \equiv 1 \pmod{10} \\
2 & \equiv 4 \pmod{10} \\
3 & \equiv 9 \pmod{10} \\
4 & \equiv 6 \pmod{10} \\
5 & \equiv 5 \pmod{10} \\
6 \equiv -4 \pmod{10} & \equiv 6 \pmod{10} \\
7 \equiv -3 \pmod{10} & \equiv 9 \pmod{10} \\
8 \equiv -2 \pmod{10} & \equiv 4 \pmod{10} \\
9 \equiv -1 \pmod{10} & \equiv 1 \pmod{10}
\end{array}
$$

note symmetry.

#7 $a^2 - a + 7$ ends in 3, 7, or 9

$a \equiv r \pmod{10}$ $\quad r \in \{0, 1, \dots, 9\}$.

$$a^2 - a + 7 \equiv r^2 - r + 7 \pmod{10}$$

$$
\begin{array}{ll}
r = 0 & P(r) \equiv 7 \pmod{10} \\
1 & \equiv 7 \pmod{10} \\
2 & \equiv 9 \pmod{10} \\
3 & \equiv 3 \quad '' \\
4 & \equiv 9 \quad '' \\
5 & \equiv 7 \quad '' \\
6 & \equiv 7 \quad '' \\
7 & \equiv 9 \quad '' \\
8 & \equiv 3 \quad '' \\
9 & \equiv 9 \quad ''
\end{array}
$$

18 a). $N = 6923$ $\quad M = 3296$

$$N = a_m 10^m + a_{m-1} 10^{m-1} + \dots + a_2 10^2 + a_1 10 + a_0$$

$$- \quad M = a_0 10^m + a_1 10^{m-1} + \dots + a_{m-2} 10^2 + a_{m-1} 10 + a_m$$

$$N - M = \underline{(a_m - a_0)10^m + \dots + (a_2 - a_{m-2})10^2} + (a_1 - a_{m-1})10 + a_0 - a_m$$

Divisible by 9?

Add the coefficients – they cancel perfectly! – to get 0, divisible by 9.

b) Any palindrome with an even number of digits is divisible by 11.

$$6334 \qquad 6 \cdot 10^3 + 3 \cdot 10^2 + 3 \cdot 10^1 + 6$$

$$N = a_{2k+1} 10^{2k+1} + a_{2k} \cdot 10^{2k} + \dots + a_1 10^1 + a_0$$

$$\begin{aligned}
a_{2k+1} &= a_0 \\
a_{2k} &= a_1 \\
a_{2k-1} &= a_2 \\
&\vdots \\
a_{2k-n} &= a_{n+1}
\end{aligned}$$

$$\begin{aligned}
P(-1) &= a_{2k+1}(-1)^{2k+1} + a_{2k}(-1)^{2k} + \dots + (-1)^1 \cdot a_1 + a_0 \\
&= a_0 (-1)^{2k+1} + a_1 (-1)^{2k} + \dots + a_1(-1) + a_0 \\
&= a_0(1-1) + a_1(1-1) + \dots + a_k(1-1) \\
&= 0 \quad \checkmark
\end{aligned}$$

$$P(-1) \equiv P(10) \pmod{11} \equiv 0 \quad .$$