Lecture 19

Enoch Cheung

October 30, 2013

1. Consider $n = 32688048$. Clearly $2|n$ since its last digit is even.

   (a) Does $2^2|n$? Does $2^3|n$?

   Note that

   $$n = 32688000 + 48 = 326880(100) + 48 = 326880(25 \cdot 2^2) + 48$$

   so since $2^2|48$, $2^2|n$.

   Similarly,

   $$n = 32688000 + 48 = 32688(1000) + 48 = 32688(125 \cdot 2^3) + 48$$

   so since $2^3|48$, $2^3|n$.

   (b) Clearly, $10^j = (5 \cdot 2)^j = 5^j \cdot 2^j$. Therefore, given any n, we can look at the last j digits such that

   $$n = q \cdot 10^j + r = q \cdot 5^j \cdot 2^j + r$$

   so by Modular Arithemtic Lemma

   $$n \equiv 0 \pmod{2^j} \iff q \cdot 5^j \dot{2}^j \equiv 0 \pmod{2^j} \wedge r \equiv 0 \pmod{2^j}$$

   and since $q \cdot 5^j \dot{2}^j \equiv 0 \pmod{2^j}$ is always true,

   $$2^j|n \iff 2^j|r$$

   so n is divisible by 2^j if and only if the last j digits are.

   (c) By the same argument,

   $$n \equiv 0 \pmod{5^j} \iff q \cdot 5^j \dot{2}^j \equiv 0 \pmod{5^j} \wedge r \equiv 0 \pmod{5^j}$$

   so

   $$5^j|n \iff 5^j|r$$

   so n is divisible by 5^j if and only if the last j digits are.

2. (a) $100 \equiv 9 \pmod{13}$ (since $100 = 7 \cdot 13 + 9$)

   (b) $-1000 \equiv 1 \pmod{13}$ (since $-1000 = -77 \cdot 13 + 1$)

   (c) $2^{15} \equiv 8 \pmod{13}$ (By Fermat's little theorem $2^{13} \equiv 2 \pmod{13}$)

3. Construct addition and multiplication table for $\mathbb{Z}/6\mathbb{Z}$:

+	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

×	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

4. Let $m \in \mathbb{N}$. Show that if $a \equiv b \pmod{m}$ then $\gcd(a, m) = \gcd(b, m)$.

   Suppose $a \equiv b \pmod{m}$. We will show that $\gcd(a, m) \geq \gcd(b, m)$, by showing that any common divisor of b, m is also a common divisor of a, m. Suppose d is a common divisor of b, m, so $d|b$ and $d|m$. Then since $d|m$ and $m|(b-a)$, then $d|(b-a)$, and since $d|b$, then $d|-a$ so $d|a$. Therefore, d is a common divisor of a, m.

   By symmetry, we can do the same proof to show $\gcd(b, m) \geq \gcd(a, m)$. Therefore, $\gcd(a, m) = \gcd(b, m)$.