Homework 4, solutions

Sulution to problem 19. Let $a_k a_{k-1} \dots a_0$ be a decimal representation of a positive integer n. This means that $n = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \dots + a_k \cdot 10^k$, where a_i are the decimal digits of n. We can also write this as

$$n = (a_2 a_1 a_0) + (a_5 a_4 a_3) \cdot 10^3 + (a_8 a_7 a_6) \cdot (10^3)^2 + (a_{11} a_{10} a_9) \cdot (10^3)^3 \cdots ,$$

where $a_{i+2} a_{i+1} a_i = a_i + 10a_{i+1} + 100a_{i+2}$ is the three digit number formed by 3 consecutive digits of n. Now $1001 = 7 \cdot 11 \cdot 13$ means that for $p \in \{7, 11, 13\}$ we have $10^3 \equiv -1 (\mod p)$. Thus

$$n = (a_2 a_1 a_0) + (a_5 a_4 a_3) \cdot 10^3 + (a_8 a_7 a_6) \cdot (10^3)^2 + (a_{11} a_{10} a_9) \cdot (10^3)^3 \cdots \equiv$$

$$\equiv (a_2 a_1 a_0) - (a_5 a_4 a_3) + (a_8 a_7 a_6) - (a_{11} a_{10} a_9) + \cdots (\mod p).$$

For example,

$$123456789 \equiv 789 - 456 + 123 = 456 (\mod 13).$$

This observation provides a fairly fast algorithm to raplace a given number by a congruent three digit number when the modulus is $7, 11$, or 13 (or any other divisor of 1001). The three digit number has to be then further reduced by hand. In the example above, we see that $456 \equiv 1 (\mod 13)$.

Solution to problem 21. We have $(172195)(572167) = 985242x6565$. We will work modulo 11 and use what we learned in class (see problem 18 in the book). We have

$$172195 \equiv 5-9+1-2+7-1 = 1 (\mod 11), \quad 572167 \equiv 7-6+1-2+7-5 = 2 (\mod 11),$$

and

$$985242x6565 \equiv 5 - 6 + 5 - 6 + x - 2 + 4 - 2 + 5 - 8 + 9 = 4 + x (\mod 11).$$

It follows that $4 + x \equiv 1 \cdot 2 = 2 (\mod 11)$, i.e. $x \equiv -2 (\mod 11)$. The only digit which satisfies this congruence is $x = 9$.

Solution to problem 26. a) The congruence $a^2 \equiv b^2 (\mod p)$ means that

$$p | (a^2 - b^2) = (a - b)(a + b).$$

Since p is a prime number, Euclid's Lemma tells us that either $p|(a-b)$ or $p|(a+b)$. The first case says $a \equiv b(\mod p)$, the second case says $a \equiv -b(\mod p)$. In other words, $a \equiv \pm b(\mod p)$.

b)We use same reasoning as in a). We have $p|(a^2 - a) = a(a-1)$, so either $p|a$ or $p|(a-1)$ (by Euclid's Lemma). Thus either $a \equiv 0(\mod p)$ or $a \equiv 1(\mod p)$.

Remark. The above argument easily extends to the following general result (equivalent to Euclid's Lemma):
if p is a prime and $ab \equiv 0(\mod p)$ the either $a \equiv 0(\mod p)$ or $b \equiv 0(\mod p)$.

Read section 2.1 in the book. Solve problems 19, 21, 26 to section 2.1.