Stony Brook University
MAT 118 Spring 2013

Modular Arithmetic

UPC code again.

When working with the UPC check-digit system, we learned that if any one of the twelve digits in a UPC number is lost, it can be reconstructed from the rest. For example suppose the fifth digit of the code on my box of chalk was illegible, so it reads $0720x7311450$. The check digit is calculated so that the sum of all the digits, multiplied alternately by 3 and by 1, is a multiple of 10 ("congruent to 0 *mod* 10"). That sum turns out to be

$$3\cdot 0+1\cdot 7+3\cdot 2+1\cdot 0+3\cdot x+1\cdot 7+3\cdot 3+1\cdot 1+3\cdot 1+1\cdot 4+3\cdot 5+1\cdot 0$$

giving

$$52+3\cdot x\equiv 0 \ \ mod\ 10.$$

Since an equivalence *mod* 10 still holds if we add or subtract 10 from either side, we can break 52 as $50+2$ and discard the 50; this leaves

$$2+3\cdot x\equiv 0 \ \ mod\ 10,$$

so what is x? Adding 10 to the right gives $2+3\cdot x\equiv 10$ *mod* 10, and subtracting 2 *from both sides* gives $3\cdot x\equiv 8$ *mod* 10. Then the "threes" multiplication table *mod* 10 shows that x must be equivalent to 6 *mod* 10. Since x is a positive single digit, it must be exactly 6.

The UPC code can retrieve a lost digit in the fifth place because we can solve the equation $a+3\cdot x\equiv 0$ *mod* 10 or, equivalently, $3\cdot x\equiv 10-a$ *mod* 10 no matter what a is. This is only possible because 3 and 10 have no common factors. As we have checked in class, one cannot solve $2\cdot x\equiv 1$ *mod* 10, and $2\cdot x\equiv 4$ *mod* 10 has two distinct solutions, so would not help in retrieving lost digits.

When the modulus is a prime number.

Suppose that instead of 10 we were solving equations *mod* 11. Since 11 is a prime, the only way for a number to have a factor in common with 11 is to be a multiple of 11, i.e. to be $\equiv 0$ *mod* 11. So for any number k which is not a multiple of 11, we can always solve an equation like $k\cdot x\equiv a$ *mod* 11. The ks that work are thus $1,2,3,4,5,6,7,8,9,10$ and any number equivalent to them *mod* 11 .

- For typographical economy let's use 1 for the equivalence class of 1 *mod* 11, etc. So 1 represents the set of all integers congruent to 1 *mod* 11, i.e. $\{\ldots -21, -10, 1, 12, 32, \ldots\}$.

One way to see how to solve congruence equations is to start with the multiplication table *mod* 11, using our new notation. Here is how the equivalence classes multiply. To multiply $10 \cdot 9$ we take any representative of 10 and any representative of 9, multiply them as integers, and take the remainder after the product is divided by 11. The obvious choices are 10 and 9; then since $90 = 8 \cdot 11 + 2$ our rule gives $10 \cdot 9 = 2$. But note that we could have taken $32 = 2 \cdot 11 + 10$ as a representative for 10 and $64 = 5 \cdot 11 + 9$ as a representative for 9. The product $32 \cdot 64 = 2048$ is equal to $196 \cdot 11 + 2$, i.e. the equivalence class *mod* 11 of 2048 is 2, the same answer we got for 10 and 9.

- Why does this work? Any representative for 10 is 10 plus a multiple of 11, so it has theform $k \cdot 11 + 10$ for some whole number k (which can be positive, zero or negative). Similarly any representative for 9 is 9 plus a multiple of 11, so it has theform $\ell \cdot 11 + 9$ for some whole number ℓ. Multiplying the representatives together gives $(k \cdot 11 + 10) \cdot (\ell \cdot 11 + 9)$ which is $k \cdot 11 \cdot \ell \cdot 11 + k \cdot 11 \cdot 9 + 10 \cdot \ell \cdot 11 + 10 \cdot 9$. Grouping together all the multiples of 11 gives $(k \cdot 11 \cdot \ell + k \cdot 9 + 10 \cdot \ell) \cdot 11 + 90$ and since $90 = 8 \cdot 11 + 2$ our product becomes $(k \cdot 11 \cdot \ell + k \cdot 9 + 10 \cdot \ell + 8) \cdot 11 + 2$, with equivalence class 2, independently of k and ℓ.

Here is our multiplication table:

$\cdot$	0	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10
2	0	2	4	6	8	10	1	3	5	7	9
3	0	3	6	9	1	4	7	10	2	5	8
4	0	4	8	1	5	9	2	6	10	3	7
5	0	5	10	4	9	3	8	2	7	1	6
6	0	6	1	7	2	8	3	9	4	10	5
7	0	7	3	10	6	2	9	5	1	8	4
8	0	8	5	2	10	7	4	1	9	6	3
9	0	9	7	5	3	1	10	8	6	4	2
10	0	10	9	8	7	6	5	4	3	2	1

Notice that in each row all the products are different. This happens for the following reason. Suppose that $7 \cdot 7 = 7 \cdot 3$. Subtracting $7 \cdot 3$ from both sides gives $7 \cdot 7 - 7 \cdot 3 = 0$ or $7 \cdot 4 = 0$. But this would mean that $7 \cdot 4$ was 11 or a multiple of 11, so 11 would divide $7 \cdot 4$ which is impossible. (Based on the principle: if a prime divides the product of two numbers, it must divide one of the factors). This paragraph explains why $7 \cdot 7 = 7 \cdot 3$ is impossible; the same argument works to show that $7 \cdot a = 7 \cdot b$ for $a \neq b$ between 0 and 10.

Since there are 10 elements in each row, and all are different, the row must contain the elements $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10$ in some order. This gives an elementary way to solve an equation like $5 \cdot x \equiv 2 \ \ mod \ 11$, or $5 \cdot x = 2$: we look along the 5 row until we find 2; it is in the column corresponding to 7, so the solution is $x = 7$, or $x \equiv 7 \ \ mod \ 11$.