Week 3, lecture 1:
Applications of modular arithmetic.
Inverses modulo m

MA180/185/190 Algebra

Angela Carnevale

Applications

Credit card numbers

PPS numbers

Division modulo m

Recap

→ $a \equiv b \pmod{m}$ if $a-b$ is an integer multiple of m

$34 \equiv 13 \pmod{7}$

both 34 and 13 are also congruent to 6 mod 7

→ $a+b \equiv c \pmod{m}$ if $a+b-c$ is int. mult. of m

→ $a \cdot b \equiv c \pmod{m}$ if $a \cdot b - c$ is int mult of m.

Note We've seen that sometimes multiplying non-zero numbers together give us something congruent to 0 mod m.

$3 \cdot 5 \equiv 0 \pmod{15}$

Back to our challenge!

Recall another of our challenges

On our credit card, one digit faded away. We can currently see:

5457 6238 9?23 4113

What's the missing digit? Let's call the missing digit x

Using the sumcheck criterion from Lecture 4, we get the following

$$\underline{1}+4+\underline{1}+7+\underline{3}+2+\underline{6}+8+\underline{9}+x+\underline{4}+3+\underline{8}+1+\underline{2}+3 \equiv 0 \pmod{10}$$

(Recall: the underlined digits are obtained by multiplying by 2 the corresponding digit in the credit card number and, if the resulting number is made of 2 digits, we add them up.)

So $x+62 \equiv 0 \pmod{10}$ telling us that the missing digit is $\underline{\underline{8}}$

PPS numbers

A PPS number[1] is a code that uniquely identifies a tax resident in the Republic of Ireland. It is made up of 9 digits: 7 numbers between 0 and 9 and 2 letters between **A** and **W**. For example

1234567FA

is a valid PPS number.

The first of the two letters (F in our example) is a **check digit**: it can be obtained from the remaining 8 with some operations **modulo** 23.

First, we translate (back and forth) between letters and numbers by associating with each letter the position it occupies in the alphabet. So $A \leftrightarrow 1$, $B \leftrightarrow 2$, $\ldots V \leftrightarrow 22$ and $W \leftrightarrow 23$.

[1] here we will discuss the post-2013 version

PPS numbers

Let's call d_1, $d_2 \ldots, d_9$ the digits of the PPSn. We associate to each position/digit some "weights" as follows:

Weight	8	7	6	5	4	3	2	1	9
Digit	d_1	d_2	d_3	d_4	d_5	d_6	d_7	d_8	d_9

1 2 3 4 5 6 7 F A

PPS numbers

Let's call d_1, $d_2 \dots, d_9$ the digits of the PPSn. We associate to each position/digit some "weights" as follows:

Weight	8	7	6	5	4	3	2	1	9
Digit	d_1	d_2	d_3	d_4	d_5	d_6	d_7	d_8	d_9

We then multiply the digits $d_1, \dots, d_7$ and d_9 by their weight and add up all the resulting numbers.

The **check digit** d_8 should be equal to remainder of this **modulo** 23:

$$d_8 \equiv 8 \cdot d_1 + 7 \cdot d_2 + 6 \cdot d_3 + 5 \cdot d_4 + 4 \cdot d_5 + 3 \cdot d_6 + 2 \cdot d_7 + 9 \cdot d_9 \pmod{23}$$

PPS numbers

Let's check that the 9-digit code from before is a valid PPS number:

Weight	8	7	6	5	4	3	2	1	9
Digit	1	2	3	4	5	6	7	F	A

$= 1$

We first consider all the digits (and their weights) except the check digit d_8. Remember: we "translate" letters into numbers by their position in the alphabet so $A = 1$

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

$$8 + 14 + 18 + 20 + 20 + 18 + 14 + 9 = 121$$

We then compute the remainder of 121 mod 23 which gives us 6

That is, the check digit should be the 6th letter of the alphabet, and indeed it is F. ✓

PPS numbers

Suppose now we are missing the last digit from a PPS number. For instance, we have

$$1213001W?$$

We can try to find out what the missing digit ? should be:

we call x the missing digit and apply the sum check. It tells us that the following congruence should be satisfied

$$8\cdot 1+7\cdot 2+6\cdot 1+5\cdot 3+4\cdot 0+3\cdot 0+2\cdot 1+9\cdot x\equiv 1\cdot 23\equiv 0 \pmod{23}$$

working out the operations we get

$$9x+45$$

now, we know that on the 23-hour clock $45\equiv 22$ so we can write $9x+22\equiv 0 \pmod{23}$ which we can rewrite as $9x\equiv -22 \pmod{23}$ and again bringing -22 on the 23-hour clock we get that $9x\equiv 1 \pmod{23}$ should hold. How can we solve this congruence?

Back to gcds

We would like to find a number x in $\mathbb{Z}_{23}$ such that

$$\boxed{9 \cdot x \equiv 1 \pmod{23}} \qquad (*)$$

Let's go back to gcds and Bézout's theorem. Since 9 and 23 are coprime, we can find integers x and y such that

$$9 \cdot x + 23y = 1$$

If this equation holds, then it holds also as a congruence modulo 23! But modulo 23, the term "$23y$" will be congruent to 0.... That will help us find x to solve the congruence $(*)$

Back to gcds

We observed that $\gcd(23,9)=1$ but let's use Euclid's algorithm to find x and y.

$$\left.\begin{aligned} 23 &= 9\cdot 2+5 \\ 9 &= 5\cdot 1+4 \\ 5 &= 4\cdot 1+1 \\ 4 &= 4\cdot 1+0 \end{aligned}\right\}$$

We now use these identities (with back substitution) to write 1 as an integer combination of 23 and 9. You can go back to the notes from Lecture 2 and Lecture 3 for more examples.

$$\begin{aligned} 1 &= 5-4\cdot 1 \\ &= 5-(9-5\cdot 1) = 5-9+5 = 5\cdot 2-9 \\ &= (23-9\cdot 2)\cdot 2-9 = 23\cdot 2-9\cdot 5 \end{aligned}$$

So $23\cdot 2+9\cdot(-5)=1$ but "mod 23" the first term is congruent to 0, giving us $9\cdot(-5)\equiv 1 \pmod{23}$.

The missing digit

Now $9 \cdot (-5) \equiv 1 \pmod{23}$

tells us that $x \equiv -5 \equiv 18 \pmod{23}$ is the "missing digit", or better, the missing digit is the 18^{th} letter of the alphabet, namely R. The complete PPS number is

$$\boxed{1213001WR}$$

As an exercise, you can now verify that 1213001*WR* is a valid PPS number.