

THE JOY OF NUMBERS

1. CONGRUENCE AND ADDITION

Based on the examples from last time, and on more examples we decided that it was time for a theorem:

(1.1) **Theorem.** Let $a \equiv x \pmod{m}$ and $b \equiv y \pmod{m}$. Show that

- (1) $a + b \equiv x + y \pmod{m}$;
- (2) $a - b \equiv x - y \pmod{m}$;
- (3) $a \cdot b \equiv x \cdot y \pmod{m}$;

What is interesting about this theorem is that if it is true then we can define an addition, a subtraction and a multiplication for these sets $[x]$ (which by the way we decided to call equivalence classes). For example we can say that $[a] + [b] = [a + b]$. This makes sense, because if I choose another element a as a representative of the class $[x]$ ($a \in [x]$) and another element b as representative of the class $[y]$ ($b \in [y]$), then $[a] + [b] = [a + b] = [x + y] = [x] + [y]$. So my definition of addition is representative-free. I was not finished writing these things down when Chris said that we can also say something about the division. But what? The statement $\frac{a}{b} \equiv \frac{x}{y} \pmod{m}$ does not make much sense, as Matt and Alex observed. In general $\frac{a}{b}$ is not an integer. But we noticed that we can re-state the division in the following way $\frac{a}{b} = x$ if $xb = a$. So does it make sense to have division between classes as it does the addition? Let's do the usual: compute some examples:

(1.2) **Example.** Let $m = 5$. Consider the equivalence class of 9 and the equivalence class of 7. If $\frac{[9]}{[7]}$ exists it is some class $[x]$, such that $[x] \cdot [7] = [9]$. Can we find an integer x such that $7x \equiv 9 \pmod{5}$? Emil, was super fast, and she noticed that $2 \cdot 7 \equiv 9 \pmod{5}$. OK, maybe we were lucky. Let's try another one.

(1.3) **Example.** Let $m = 5$. What is $\frac{[4]}{[3]}$? If there is such a thing, it should be an equivalence class $[x]$ corresponding to some integer x such that $3x \equiv 4 \pmod{5}$. Again $3 \cdot 3 = 9 \equiv 4 \pmod{5}$

It seems like that with $m = 5$ we can divide. Let's try with another m .

(1.4) **Example.** $m = 4$. can we find an equivalent class $[x]$ such that $\frac{[3]}{[2]} = [x]$? Sara said no. Finding such an x would mean that $2x \equiv 3 \pmod{4}$, which means that there exists an integer h such that $2x - 3 = 4h$. But this would imply that 3 is an even number which is a contradiction. So, we cannot divide $[3]$ by $[2]$.

Can't we ever divide if $m = 4$.

(1.5) **Example.** Let $m = 4$. Does it make sense $\frac{[5]}{[3]}$. Can we find an integer x such that $[3][x] = [5]$? Yes, infact $3 \cdot 3 = 8 \equiv 5 \pmod{4}$.

Date: October 16, 2007.

When is it that we can divide? Let's think about this for next time. And now we go back to the proof of the Theorem 1.1:

Theorem 1.1(1). (Matt). We know that $m \mid a - x$ and $m \mid b - y$, which means that there exist integers h and k such that $a - x = hm$ and $b - y = km$. If we sum the two equalities, we get $(a + b) - (x + y) = m(h + k)$, which says that $a + b \equiv x + y \pmod{m}$. \square

Class was half way and i wanted you guys to start having some fun computing. I need the following

(1.6) **Proposition.** Let $a \equiv b \pmod{m}$ then $a^n \equiv b^n \pmod{m}$ for every positive integer n .

Proof. (Eric). By induction on n . $P(1)$: $a \equiv b \pmod{m}$, is true by the hypothesis. Let's assume that $P(n)$ holds, so that $a^n \equiv b^n \pmod{m}$. We need to prove $P(n+1)$, which means that we need to prove $a^{n+1} \equiv b^{n+1} \pmod{m}$. Since $P(n)$ holds then we know that there exists an integer h such that $a^n - b^n = hm$. If we multiply both side by a , we obtain

$$(1.6.1) \quad a^{n+1} - ab^n = ham.$$

We also know that $P(1)$ holds and in particular there exists an integer k such that $a - b = km$ and $a = b + km$. If we substitute such expression of a in the equation 1.6.1, we obtain

$$a^{n+1} - (b + km)b^n = ham, \quad \text{which implies} \quad a^{n+1} - b^{n+1} = m(ha + kb^n),$$

which give us the desired conclusion. Very nice Matt. \square

Recall that we denote by $25\%3$ the smallest positive integer congruent to 25 modulo 3. So in particular $25\%3 = 1$. Here is the fun:

(1.7) **Example.** Compute $271816212\%5$. You guys are really fast: $271816212\%5 = 2$.

(1.8) **Example.** Compute $(371812) \cdot (876123)\%5$. Also here the answer came pretty fast. $(371812) \cdot (876123)\%5 = 1$.

(1.9) **Example.** Compute $(47) \cdot (23)\%7$. The answer came a little bit later. But $47 \equiv 5 \pmod{7}$ and $23 \equiv 2 \pmod{7}$ and therefore $(27) \cdot (23) \equiv (5) \cdot (2) \equiv 3 \pmod{7}$.

(1.10) **Example.** Compute $5^{47} \pmod{21}$. This one was hard. We noticed that $5^2 = 25 \equiv 4 \pmod{21}$. Therefore $5^4 = (5^2)^2 \equiv 4^2 \equiv (-5) \pmod{21}$. It follows that

$$5^8 = (5^2)^4 \equiv 4^4 \equiv (4^2)^2 \equiv (-5)^2 \equiv 4 \pmod{21}.$$

so we have that

$$5^8 \equiv 4^4 \equiv 4 \pmod{21}.$$

So we obtain

$$\begin{aligned} 5^{47} &= 5^{40+7} = 5^{8+8+8+8+8+7} = 5^8 5^8 5^8 5^8 5^8 5^7 \\ &\equiv 4 \cdot 4 \cdot 4 \cdot 4 \cdot 4 \cdot 5^{2+2+2+1} \\ &\equiv 4^4 \cdot 4 \cdot 5^2 5^2 5^2 5 \equiv 4^4 \cdot 4 \cdot 4 \cdot 4 \cdot 4 \cdot 5 \\ &\equiv 4 \cdot 4^4 \cdot 5 \equiv 4 \cdot 4 \cdot 5 \equiv (-5)(5) \equiv -4 \pmod{21} \end{aligned}$$