

MATH221-001 200630 Problem Set 6 Solutions DRAFT

Edward Doolittle

December 4, 2006

1. (a) $100 = 13 \times 7 + 9$ so $100 \pmod{13} = 9$.
(b) $123456789 \equiv 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 = 36 \equiv 3 + 6 = 9 \equiv 0 \pmod{9}$ so the residue is 0 modulo 9.
(c) $9652 = 9000 + 652 \equiv 652 \pmod{1000}$.
(d) $123456789 \equiv 9 - 8 + 7 - 6 + 5 - 4 + 3 - 2 + 1 = 5 \pmod{11}$.
2. (a) We have $17263 \equiv 3 \pmod{10}$ and $19274 \equiv 4 \pmod{10}$ so $17263 \times 19274 \equiv 3 \times 4 = 12 \equiv 2 \pmod{10}$.
(b) $392 \times 36127 \equiv 2 \times 2 \equiv 4 \equiv -1 \pmod{5}$.
(c) $2366 \times 5003 \equiv 16 \times 3 \equiv 48 \equiv -2 \pmod{25}$.
(d) $839 \times 5923 \equiv 39 \times 923 \equiv 7 \times 123 \equiv 7 \times 3 = 21 \equiv 13 \pmod{8}$.
3. (a) We have $3 \equiv 3 \pmod{10}$, $3^2 \equiv 9 \pmod{10}$, $3^3 \equiv 27 \equiv 7 \pmod{10}$, $3^4 \equiv 3 \times 3^3 \equiv 3 \times 7 \equiv 21 \equiv 1 \pmod{10}$ so the last digit of 3^4 is 1. Note that we saved ourselves a certain amount of effort by working modulo 10, but that we could have easily answered this question by first finding 3^4 and then taking the last digit.
(b) Here, finding 7^{40} is infeasible, even with a calculator. But we have

$$\begin{aligned}7^0 &\equiv 1 \pmod{10} \\7^1 &\equiv 7 \pmod{10} \\7^2 &\equiv 49 \equiv 9 \pmod{10} \\7^3 &\equiv 7 \times 7^2 \equiv 7 \times 9 \equiv 63 \equiv 3 \pmod{10} \\7^4 &\equiv 7 \times 7^3 \equiv 7 \times 3 \equiv 1 \pmod{10} \\7^5 &\equiv 7 \pmod{10} \\7^6 &\equiv 9 \pmod{10} \\7^7 &\equiv 3 \pmod{10} \\7^8 &\equiv 1 \pmod{10}\end{aligned}$$

with the pattern repeating in a cycle of 4. Therefore we can conclude that $7^{40} \equiv 7^{36} \equiv \dots \equiv 7^4 \equiv 7^0 \equiv 1 \pmod{10}$, in other words that the last digit of 7^{40} is 1.

- (c) This one is actually easy: we have $217 \equiv 7 \pmod{10}$ so $217^{40} \equiv 7^{40} \equiv 1 \pmod{10}$.

(d) We have

$$\begin{aligned}2^0 &\equiv 1 \pmod{10} \\2^1 &\equiv 2 \pmod{10} \\2^2 &\equiv 4 \pmod{10} \\2^3 &\equiv 8 \pmod{10} \\2^4 &\equiv 6 \pmod{10} \\2^5 &\equiv 2 \pmod{10} \\2^6 &\equiv 4 \pmod{10} \\2^7 &\equiv 8 \pmod{10} \\2^8 &\equiv 6 \pmod{10} \\2^9 &\equiv 2 \pmod{10}\end{aligned}$$

and so on. The pattern repeats in a cycle of 4, but only from 2^1 onwards, so we have to be a little more careful here. We have $2^{157} \equiv 2^{153} \equiv 2^{149} \equiv \dots \equiv 2^9 \equiv 2 \pmod{10}$. We don't go as far as we can because the pattern might change. (It doesn't in this case, but I can cook up examples; e.g., find the last two digits of 6^{201} .)

4. (a) We have $8,901 \equiv 8 + 9 + 0 + 1 \equiv 8 + 1 \equiv 0 \pmod{9}$ so the entire left hand side must be congruent to $0 \pmod{9}$. Since the right hand side is also congruent to $0 \pmod{9}$, casting out 9s doesn't tell us anything. (In fact, the multiplication is incorrect, there being a transposition error in digits 4 and 5.)
 - (b) The left hand side is $9787 \times 1258 \equiv 787 \times 25 \equiv 4 \times 7 \equiv 28 \equiv 1 \pmod{9}$ while the right hand side is $12310046 \equiv 746 \equiv 710 \equiv 8 \pmod{9}$, so casting out 9s indicates that there's an error in this multiplication.
 - (c) $6893 \times 16922 \equiv 8 \times 74 \equiv 8 \times 11 \equiv 8 \times 2 \equiv 7 \pmod{9}$ while $115543346 \equiv 21074 \equiv 5 \pmod{9}$ so this multiplication is incorrect.
 - (d) $5783 \times 40162 \equiv 1283 \times 4 \equiv 5 \times 4 \equiv 20 \equiv 2 \pmod{9}$ while $232256846 \equiv 5411126 \equiv 2 \pmod{9}$, so casting out 9s doesn't give us a definitive answer, only that the multiplication may be correct. In fact, the multiplication is correct.
5. (a) $52739253 \equiv 5 + (2 + 7) + 3 + (9) + 2 + 5 + 3 \equiv 5 + 3 + 2 + 5 + 3 \equiv 8 + 2 + 8 \equiv 18 \equiv 0 \pmod{9}$ so the number is divisible by 9 and is not prime.
 - (b) $391391 \equiv 1 - 9 + 3 - 1 + 9 - 3 \equiv 0 \pmod{11}$ so the number is divisible by 11 (and is bigger than 11) so is not prime.
 - (c) $39360711 \equiv 7 + 1 + 1 \equiv 9 \equiv 0 \pmod{3}$ so the number is divisible by 3 (and is bigger than 3) so is not prime.
 - (d) $19392329 \equiv 9 - 2 + 3 - 2 + 9 - 3 + 9 - 1 \equiv 7 + 1 + 6 + 8 \equiv 22 \equiv 0 \pmod{11}$ so the number is divisible by 11 (and is bigger than 11) so is not prime.
6. Assume that there are non-zero x, y, z, w satisfying the equation. If there are any factors common to all of those numbers (e.g., if they are all even), then we can divide through by the greatest common factor and get a new solution x', y', z', w' such that there are no factors common to all four numbers. This will be our "minimal criminal".

In arithmetic modulo 3 we have $x^2 \equiv 0$ or 1 , and the same for all the other squares (just make up a table with the three possible residues for x in one column and the results for $x^2 \pmod{3}$ in the other). Note that $x^2 + y^2 = 3(z^2 + w^2) \equiv 0 \pmod{3}$; looking at all the cases (draw a table and ask me if you're having trouble), it follows that $x, y \equiv 0 \pmod{3}$ so x and y must both be divisible by 3, and we have $x = 3x_1, y = 3y_1, x^2 + y^2 = 9(x_1^2 + y_1^2) = 3(w^2 + z^2)$ which implies $w^2 + z^2 = 3(x_1^2 + y_1^2)$. By analogous reasoning, it follows that w and z are divisible by 3. However, that means all of x, y, z, w were divisible

by 3, which contradicts the assumption that they had no common factor. It follows that there were no such x, y, z, w in the first place.

You can also solve this question using infinite descent.

7. We need an even number of players, so we label the players $0, \dots, 7$ and add an eighth player ∞ which stands for a “bye”. According to the diagram we developed, we have on round n , $n = 0, \dots, 7$ that ∞ plays n , that $n - 1$ plays $n + 1$, $n - 2$ plays $n + 2$, and $n - 3$ plays $n + 3$, where all arithmetic is done modulo 7. Try to figure out what this has to do with the septagon figure I drew on the blackboard (and what that has to do with the process we enacted); ask me if you don’t understand. Could you write a computer program to generate round robin tournaments?
8. We could obtain any of these inverses by guessing or trying all possible residues, but I have chosen to use the Euclidean Algorithm in each case.
 - (a) We have $2 \times 6 - 11 = 1$ so $2 \times 6 \equiv 1 \pmod{11}$ so the inverse of 2 modulo 11 is 6.
 - (b) We have (by the Euclidean algorithm, say) $7 \times (-2) + 15 = 1$ so $7 \times -2 \equiv 1 \pmod{15}$, so an inverse for 7 modulo 15 is -2 . It’s more usual to pick least nonnegative residues, so a better answer would be that the inverse of 7 modulo 15 is $15 - 2 = 13$.
 - (c) We have

$$\begin{aligned} 16 &= 7 \times 2 + 2 \\ 7 &= 2 \times 3 + 1 \\ 2 &= 1 \times 2 \end{aligned}$$

so

$$\begin{aligned} 2 &= 16 \times 1 - 7 \times 2 \\ 1 &= 7 \times 1 - 2 \times 3 = 7 \times 1 - (16 \times 1 - 7 \times 2) \times 3 = 7 \times 7 - 16 \times 3 \end{aligned}$$

which is easy to check. It follows that $7 \times 7 \equiv 1 \pmod{16}$ so 7 is its own inverse modulo 16

- (d) We have

$$\begin{aligned} 13 &= 5 \times 2 + 3 \\ 5 &= 3 \times 1 + 2 \\ 3 &= 2 \times 1 + 1 \\ 2 &= 1 \times 2 \end{aligned}$$

so

$$\begin{aligned} 3 &= 13 - 5 \times 2 \\ 2 &= 5 - 3 \times 1 \\ 1 &= 3 - 2 \times 1 \end{aligned}$$

and $1 = 3 - 2 \times 1 = 3 - (5 - 3) = 3 \times 2 - 5 = (13 - 5 \times 2) \times 2 - 5 = 13 \times 2 - 5 \times 5$ (check). It follows that $1 \equiv 5 \times -5$ modulo 13, so an inverse for 5 modulo 13 is $-5 \equiv 8$ (check).

9. As per the above, we repeatedly divide to obtain

$$\begin{aligned} m &= r \times q_1 + r_1 \\ r &= r_1 \times q_2 + r_2 \\ &\dots \\ r_{k-2} &= r_{k-1} \times q_k + 1 \\ r_{k-1} &= 1 \times r_{k-1}. \end{aligned}$$

We then move all the remainders to one side of the above equations and repeatedly substitute one relation into another to get an expression of the form $mx + ry = 1$ for some $x, y \in \mathbb{Z}$. Taking that expression modulo m we get $ry \equiv 1 \pmod{m}$. Finally, if necessary we find the least nonnegative residue of $y \pmod{m}$; that is our inverse for r .

For 47 modulo 256 we have

$$\begin{aligned} 256 &= 47 \times 5 + 21 \\ 47 &= 21 \times 2 + 5 \\ 21 &= 5 \times 4 + 1 \\ 5 &= 1 \times 5 \end{aligned}$$

Then we have

$$\begin{aligned} 21 &= 256 - 47 \times 5 \\ 5 &= 47 - 21 \times 2 \\ 1 &= 21 - 5 \times 4 \end{aligned}$$

or

$$\begin{aligned} 21 &= 256 - 47 \times 5 \\ 1 &= 21 - (47 - 21 \times 2) \times 4 = 21 \times 9 - 47 \times 4 \end{aligned}$$

or

$$1 = (256 - 47 \times 5) \times 9 - 47 \times 4 = 256 \times 9 - 47 \times 49$$

It follows that $-47 \times 49 \equiv 1 \pmod{256}$, i.e., -49 is an inverse for 47 modulo 256; the least nonnegative inverse is $256 - 49 = 207$.

10. This is actually easier than it may appear at first. First we prove that if the equation has a solution, then b is a multiple of $\text{GCD}(a, m)$. If the equation has a solution, then $ax \equiv b \pmod{m}$, i.e., $ax - b$ is a multiple of m , i.e., $ax - b = km$, i.e., $ax - km = b$. Since $\text{GCD}(a, m)$ divides both terms on the left hand side of the last equation, it must divide b , so b must be a multiple of $\text{GCD}(a, m)$.

Next we prove that if b is a multiple of $\text{GCD}(a, m)$, then the equation has a solution. By the Euclidean Algorithm we have $\text{GCD}(a, m) = as + mt$ for some integers s and t . Since b is a multiple of $\text{GCD}(a, m)$ we have $b = k \text{GCD}(a, m)$ for some integer k . Multiplying the previous equation through by k we have $k \text{GCD}(a, m) = kas + kmt$, i.e., $b = a(ks) + m(kt)$, i.e., $b \equiv a(ks) \pmod{m}$ which implies that the equation $ax \equiv b \pmod{m}$ has a solution, namely $x = ks$.

That proves both directions of the logical equivalence, and we are done.