Math 365, 2010, Exam 1 *solutions*

David Pierce

Monday, November 8, 2010

The solutions to Problems 1 and 6, and especially the remarks on the problems, were revised on November 25, 2010.

Problem 1. *Let* $\omega = \{0, 1, 2, \dots\}$*. All variables in this problem range over* ω*. Given* a *and* b *such that* $a \neq 0$*, we define*

$$\operatorname{rem}(b, a) = r,$$

if $b = ax + r$ *for some* x*, and* $r < a$*.*

a. Prove $\operatorname{rem}(a + b, n) = \operatorname{rem}(\operatorname{rem}(a, n) + \operatorname{rem}(b, n), n)$.

b. Prove $\operatorname{rem}(ab, n) = \operatorname{rem}(\operatorname{rem}(a, n) \cdot \operatorname{rem}(b, n), n)$.

Solution. a. For $\operatorname{rem}(c, n)$, write c'. Then for some x, y, and z in ω, we have

$$a = nx + a', \qquad b = ny + b', \qquad a' + b' = nz + (a' + b')',$$

hence $a + b = n(x + y + z) + (a' + b')'$. Since $(a' + b')' < n$, we have

$$(a + b)' = (a' + b')'$$

as desired.

b. With the same notation, for some w in ω we have

$$a' \cdot b' = nw + (a' \cdot b')',$$

so for some u in ω, we have $ab = nu + a' \cdot b' = n(w + u) + (a' \cdot b')'$, and therefore (since $(a' \cdot b')' < n$) we have

$$(ab)' = (a' \cdot b')'$$

as desired.

Remark. Books VII, VIII, and IX of Euclid's *Elements* develop some of the theory of what we would call the positive integers. If we allow also a zero, but not negative numbers, then we could define

$$a \equiv b \pmod{n} \iff \operatorname{rem}(a, n) = \operatorname{rem}(b, n).$$

This problem then could be used to establish the basic facts about congruence.

Remark. A number of students used the arrow "$\Rightarrow$" in their proofs. Such usage is a bad habit, albeit a common one, even among teachers. Indeed, I learned this bad habit from somebody who was otherwise one of my best teachers. Later I unlearned the habit.

In logic, the expression $A \Rightarrow B$ means

> If A is true, then B is true.

One rarely wants to say this in proofs. Rather, one wants to say things like

> A is true, and therefore B is true.

If this is what you want to say, then you should just say it in words.

In the expression "$A \Rightarrow B$", the arrow is a verb, usually read as "implies". When somebody writes the arrow in a proof, the intended meaning seems usually to be that of "*which* implies" or "*and this* implies". But the arrow should not be loaded up with these extra meanings.

One student used the arrow in place of the equals sign "=". This usage must definitely be avoided.

Another practice that should be avoided is drawing arrows to direct the reader's eye. It should be possible to read a proof left to right, top to bottom, in the usual fashion. If you need to refer to something that came before, then just say so.

It is true that, when I grade papers, I may use arrows. This is in part because, when you see your paper, I am there to explain what I meant by the arrow, if this is necessary. But what *you* write on exam should make sense without need for additional explanation by you.

If I ask you to prove a claim, I already know the claim is true. The point is not to convince me that the claim is true, or even to convince me that *you* know the claim is true. The point is to write a proof of the claim. The point is to write the sort of thing that is found in research articles and books of mathematics, often labelled with the word *Proof.*

Problem 2. *Find integers k and ℓ, both greater than* 1*, such that, for all positive integers n,*

$$k \mid 1965^{10n} + \ell.$$

Solution. Since 1965^{10n} is odd, we can let $\boxed{\ell = 3,\ k = 2.}$

Remark. This problem is based on Exercise 6. As it is stated, the problem has many solutions.

(i) The solution given here is a special case of letting k be any number such that $1965 \equiv 1 \pmod{k}$, and then letting $\ell = 2k - 1$ (or $k - 1$ if $k > 2$).
(ii) We could also let ℓ be a factor of 1965, and then let k be a factor of ℓ.
(iii) Finally, since $11 \nmid 1965$, we have by Fermat $1965^{10} \equiv 1 \pmod{11}$, so we could let $k = 11$ and $\ell = 10$.

Problem 3. *Find two positive integers a and b such that, for all integers m and n, the integer $am - bn$ is a solution of the congruences*

$$x \equiv m \pmod{999}, \qquad\qquad x \equiv n \pmod{1001}.$$

Solution. A solution of the congruences takes the form

$$x \equiv m \cdot 1001s + n \cdot 999t \pmod{999 \cdot 1001},$$

where $1001s \equiv 1 \pmod{999}$ and $999t \equiv 1 \pmod{1001}$. So we want

$$2s \equiv 1, \qquad s \equiv 500 \pmod{999}, \qquad -2t \equiv 1, \qquad t \equiv 500 \pmod{1001}.$$

Then the solution to the original congruences is

$$x \equiv m \cdot 1001 \cdot 500 + n \cdot 999 \cdot 500 \equiv 1001 \cdot 500m - 999 \cdot 501n \pmod{999 \cdot 1001}.$$

So we can let $\boxed{a = 1001 \cdot 500,\ b = 999 \cdot 501.}$

Remark. This is just a Chinese Remainder Theorem problem with letters instead of numbers.

Problem 4. *Letting* $n = \sum_{j=1}^{408} j$, *find an integer* k *such that* $0 \leqslant k < 409$ *and*

$$408! \equiv k \pmod{n}.$$

Solution. We have $n = 409 \cdot 408/2$; also 409 is prime, so by Wilson's Theorem $408! \equiv -1 \pmod{409}$. Then $408! \equiv 408$ *modulo* both 409 and 408, hence *modulo* any divisor of the least common multiple of these. But n is such a divisor. Thus we can let $\boxed{k = 408.}$

Remark. This problem is based on Exercise 49(a). A number of people argued as follows.

> Since $408! \equiv -1\ (409)$, we must have $k \equiv -1\ (409)$. Since it is required that $0 \leqslant k < 409$, it must be that $k = 408$.

But this argument does *not* prove $408! \equiv 408\ (n)$. Maybe I made a mistake, and there is *no* k meeting the stated conditions.

Problem 5. *With justification, find an integer* n*, greater than* 1*, such that, for all integers* a*,*

$$a^n \equiv a \pmod{1155}.$$

Solution. We have $1155 = 3 \cdot 5 \cdot 7 \cdot 11$, and $\gcd(3-1, 5-1, 7-1, 11-1) = \gcd(2, 4, 6, 10) = 60$. Then we can let $\boxed{n = 61.}$ Indeed, by Fermat,

- If $3 \nmid a$, then $a^2 \equiv 1\ (3)$, so $a^{60} \equiv 1\ (3)$.
- If $5 \nmid a$, then $a^4 \equiv 1\ (5)$, so $a^{60} \equiv 1\ (5)$.
- If $7 \nmid a$, then $a^6 \equiv 1\ (7)$, so $a^{60} \equiv 1\ (7)$.
- If $11 \nmid a$, then $a^{10} \equiv 1\ (11)$, so $a^{60} \equiv 1\ (11)$.

Therefore, for all a, we have $a^{61} \equiv a$ *modulo* any of 3, 5, 7, and 11, hence *modulo* their least common multiple, which is 1155.

Remark. This problem is related to Exercise 43 and our discussion of absolute pseudoprimes.

Problem 6. *Let* $\mathbb{N} = \{1, 2, 3, \dots\}$*. Suppose all we know about this set is:*

(i) proofs by induction are possible;

(ii) addition can be defined on $\mathbb{N}$*, and it satisfies*

$$x + y = y + x, \qquad\qquad x + (y + z) = (x + y) + z;$$

(iii) multiplication can be defined by

$$x \cdot 1 = x, \qquad\qquad x \cdot (y + 1) = x \cdot y + x.$$

Prove

$$x \cdot y = y \cdot x.$$

Solution. We use induction on y. As the base step, we show $x \cdot 1 = 1 \cdot x$ for all x. We do *this* by induction: Trivially, $1 \cdot 1 = 1 \cdot 1$. Suppose, as an inductive hypothesis, $x \cdot 1 = 1 \cdot x$ for some x. Then

$$\begin{aligned}
1 \cdot (x + 1) &= 1 \cdot x + 1 && \text{[by definition of multiplication]}\\
&= x \cdot 1 + 1 && \text{[by inductive hypothesis]}\\
&= x + 1 && \text{[by definition of multiplication]}\\
&= (x + 1) \cdot 1. && \text{[by definition of multiplication]}
\end{aligned}$$

By induction then, $x \cdot 1 = 1 \cdot x$.

Next we assume $x \cdot y = y \cdot x$ for all x, for some y, and we prove $x \cdot (y+1) = (y+1) \cdot x$. We do *this* by induction on x. By what we have already shown, $1 \cdot (y + 1) = (y + 1) \cdot 1$. Suppose, as an inductive hypothesis, $x \cdot (y + 1) = (y + 1) \cdot x$ for some x. Then

$$\begin{aligned}
(x + 1) \cdot (y + 1) &= (x + 1) \cdot y + x + 1 && \text{[by definition of multiplication]}\\
&= y \cdot (x + 1) + x + 1 && \text{[by the first inductive hypothesis]}\\
&= y \cdot x + y + x + 1 && \text{[by definition of multiplication]}\\
&= x \cdot y + x + y + 1 && \text{[by the first inductive hypothesis]}\\
&= x \cdot (y + 1) + y + 1 && \text{[by definition of multiplication]}\\
&= (y + 1) \cdot x + y + 1 && \text{[by the second inductive hypothesis]}\\
&= (y + 1) \cdot (x + 1). && \text{[by definition of multiplication]}
\end{aligned}$$

This completes the proof that $x \cdot (y + 1) = (y + 1) \cdot x$ for all x. *This* completes the proof that $x \cdot y = y \cdot x$ for all x and y.

Remark. This is part of Exercise 1. I tried to write out a "first generation" proof: one you might write without thinking of how to break it into parts. A proof that is easier to follow is perhaps the "second generation" proof that goes as follows (see Lemma A.3 and Theorem A.3): First show

$$x \cdot 1 = 1 \cdot x \tag{$*$}$$

by induction on x, then show

$$(y + 1) \cdot x = y \cdot x + x \tag{$\dagger$}$$

by induction on x, and finally show $x \cdot y = y \cdot x$ by induction on x. In fact, almost all students just *assumed* that $(*)$ and $(\dagger)$ were known; but they were *not* among the propositions that the problem allowed you to use.