Math 310 Homework 4 Solutions

18. If a is <u>odd</u> and $ab \equiv ac \pmod 8$, then $b \equiv c \pmod 8$

$ab \equiv ac \pmod 8$ <u>means</u> $8 \mid ac-ab$, i.e. $8 \mid a(c-b)$.

But since a is odd and the divisors of 8 are $1, 2, 4$, and 8, the <u>only</u> one which divides a is 1, so $(a, 8) = 1$. So we have $8 \mid a(c-b)$ and $(8, a) = 1$, <u>so</u> $8 \mid c-b$, i.e.,

$b \equiv c \pmod 8$.

The basic point is that all divisors of 8, besides 1, are <u>even</u>, and so they never divide a. The same would be true of any other power of 2, i.e.g. 16, 32, 64, 128, ...

19. If $a_i \equiv 1 \pmod m$ for $1 \le i \le n$, then $a_1 \cdots a_n \equiv 1 \pmod m$.

By induction on n:

$n=1$ $\quad a_1 \equiv 1 \pmod m$ so $a_1 \equiv 1 \pmod m$!

Suppose $a_1 \cdots a_n \equiv 1 \pmod m$ when $a_i \equiv 1 \pmod m$ $1 \le i \le n$, and suppose $a_{n+1} \equiv 1 \pmod m$. <u>Then</u> -

$a_1 \cdots a_{n+1} = (a_1 \cdots a_n) \cdot a_{n+1}$; but since $(a_1 \cdots a_n) \equiv 1 \pmod m$ and $a_{n+1} \equiv 1 \pmod m$, we have

$(a_1 \cdots a_n) \cdot a_{n+1} \equiv 1 \cdot 1 \pmod m$, so $a_1 \cdots a_{n+1} \equiv 1 \pmod m$.

So, by P.M.I., If $a_i \equiv 1 \pmod m$ $1 \le i \le n$ then $a_1 \cdots a_n \equiv 1 \pmod m$.

20. If $a \underset{m}{\equiv} b$ and $n \geq 1$, then $a^n \underset{m}{\equiv} b^n$.

By induction on n: $n=1$ $a \underset{m}{\equiv} b$ then $a^1 = a^1 \underset{m}{\equiv} b^1 = b$ ✓

Suppose ~~If~~ if $a \underset{m}{\equiv} b$, then $a^n \underset{m}{\equiv} b^n$. Then if $a \underset{m}{\equiv} b$, then

$$a^{n+1} = a \cdot a^n \underset{m}{\equiv} b \cdot b^n \quad (\text{since } a \underset{m}{\equiv} b \text{ and } a^n \underset{m}{\equiv} b^n)$$
$$= b^{n+1}, \text{ so } a^{n+1} \underset{m}{\equiv} b^{n+1}.$$

So by P.M.I. if $a \underset{m}{\equiv} b$, then $a^n \underset{m}{\equiv} b^n$ for all $n \geq 1$.

21.(1): $5^{18} \underset{7}{\equiv} r$; $\quad 5^{18} = (5^2)^9 = 25^9 \underset{7}{\equiv} 4^9 = (4^3)^3 = 64^3 \underset{7}{\equiv} 1^3 = 1$

So $5^{18} = 7k + 1$ for some $k \in \mathbb{Z}$

(2): $68^{105} \underset{13}{\equiv} r$; $\quad (68)^{105} \underset{13}{\equiv} (3)^{105} = 3^{3 \cdot 35} = (3^3)^{35} \cancel{\equiv}$

$$= (27)^{35} \underset{13}{\equiv} 1^{35} = 1$$

So $68^{105} = 13k + 1$ for some $k \in \mathbb{Z}$.

(3): $6^{47} \underset{12}{\equiv} r$ $\quad 6^{47} = 6^{2 \cdot 23 + 1} = (6^2)^{23} \cdot 6 = (36)^{23} \cdot 6$

$$\underset{12}{\equiv} (0)^{23} \cdot 6 = 0$$

So $6^{47} = 12k + 0$ for some k.

22. If $a \equiv b \pmod{p}$ for <u>every</u> prime p, then $a = b$.

Let $N = |b-a|$, and choose a prime p with $p > N$

Then $a \equiv b \pmod{p}$ means $b - a = pX$ for some $X \in \mathbb{Z}$,

~~i.e., $p \mid b-a$. But this implies $p \leq |b-a| = N$!~~

(if $X \geq 1$)

~~each~~ which implies $|b-a| \geq p^{\beta}$ or $X=0$. $|b-a| = N \geq p$ violates our choice of p, so we must have $X=0$, i.e. $b-a = p \cdot 0 = 0$, i.e. $a=b$. //

H3: If $n = 4m+3$, then n has a prime factor $p = 4k+3$.

~~Suppose not~~ Nah. How about by complete induction?
$m=0$: $n = 4 \cdot 0 + 3 = 3$ has prime factor $3 = 4 \cdot 0 + 3$.
If $n = 4m+3$ is prime, we're done. So suppose

$n = ab$ with $a,b \geq 2$. Since $n = 4m+3 = 2(2m+1)+1$ is odd, both a and b are odd.
Claim: Either a or b is $\equiv 3 \pmod 4$. Because:
the only alternative is that both are $\equiv 1 \pmod 4$ [if either is $\equiv_4 0$ or $\equiv_4 2$, then it is even.] But $a \equiv 1 \pmod 4$ and $b \equiv 1 \pmod 4$ implies $n = ab \equiv 1 \cdot 1 = 1 \pmod 4$, contradiction.
So either $a \equiv_4 3$ or $b \equiv_4 3$, WLOG $a \equiv_4 3$. But since $b \geq 2$, $a < n$, so $a = 4s+3$ with $s < m$. So by the inductive hypotheses, a has a prime factor $p = 4k+3$, some k.
But then $n = ab = (pX)b = p(Xb)$ so $p = 4k+3$ is a prime factor of n, as desired.
So by complete induction the result follows

There are infinitely-many primes of the form $4k+3$.

Suppose there aren't; suppose $p_1, \ldots, p_n$ are the only primes of the form $4k+3$.
Set $N = p_1 \cdots p_n$; this is a product of odd numbers

So (~~the~~ problem #19! each is $\equiv 1 \pmod 2$ so) their product is odd. So $p_1 \cdots p_n \equiv 1$ or $3 \pmod 4$.

If $p_1 \cdots p_n \underset{4}{\equiv} 1$, then look at $M = N+2 = p_1 \cdots p_n + 2$ then $M \underset{4}{\equiv} 1+2=3$, so by our previous work, M has a prime factor $p = 2k+3$. But then $p = p_i$ for some i so $p \mid N$ and $p \mid M$ so $p \mid M-N = 2$, so $p = 1$ or 2, neither of which is $\underset{4}{\equiv} 3$. Contrad. So we can't have $p_1 \cdots p_n \underset{4}{\equiv} 1$.

So we must have $p_1 \cdots p_4 \underset{4}{\equiv} 3$. But then look at $M = N+4 = p_1 \cdots p_4 + 4$. Then $M \underset{4}{\equiv} 3+4 \underset{4}{\equiv} 3$, so, again, $M = pX$ for some prime $p = 2k+3$. But then $p = p_i$ for some i, so $p \mid N$ and $p \mid M$, so $p \mid M-N = 4$, so $p = 1, 2,$ or 4, none of which are $\underset{4}{\equiv} 3$! Contrad.

So there can't be only finitely many primes $p = 4k+3$ (so that we can't make a list), so there are infinitely many primes of the form $4k+3$. ///