Sean Shu (sys3bb)
Brian Barbu (Brb9da)

40-2.5=37.5

Problem Set #6

1) prove that 3, 5, and 7 are the only prime numbers of the form p, p+2, and p+4
if we let p be greater than 3, we have that p is either one more than the multiple of 3 or 2 more than the multiple of 3
(because if any other case, then it won't be prime)

So in case 1 if p is one more than a multiple of 3, we have that p+2 results in a multiple of 3, a non-prime number, which is a contradiction

In case 2 if p is 2 more than a multiple of 3, p+4 results in a multiple of 3, which is also a contradiction.

Therefore... 3, 5, and 7 are the only prime numbers of the form p, p+2, p+4.

→

2) a. Let p be a prime number and a and b be integers. if $p|ab$, then $p|a$ or $p|b$

we can assume p divides ab. So $d = \gcd(ab, p)$
to prove $p|a$ or $p|b$ we can split into 2 cases:

$p|a$: in this case we have $k = \gcd(a, p)$
so k must either equal one or p. Where
if $k=1$ then a and p are prime, or if
$k=p$, then a equals one.

$p|b$: this case follows exactly the same as
above so let $m = \gcd(b, p)$, so m must
equal 1 or p, where if $m=1$ then $b=p$
or if $m=p$ then $b=1$

So based on the above if we know that
$p|ab$, and p is a prime number, then
p must be a factor in either a or b. The product
ab is a multiplication of a and b's factors. Since p
is definitely a factor in a times b, it must be a
factor of either a or b. Therefore, if
$p|ab$, then $p|a$ or $p|b$.

2.) b. Let p be a prime number and n an integer.
If $p|n^2$, then $p|n$
Proof by contraposition:
let $p\nmid n$, then $p\nmid n^2$
$n^2 = n \cdot n$, therefore n is clearly always a factor of n^2. if $p\nmid n$, then $n \neq pk$ where k is an integer
Since p cannot divide n, it is not a factor of n.
n^2 is the same as saying n factors multiplied by those same n factors. When $p\nmid n$, p is not a factor of n and therefore won't be a factor of n^2. so if $p\nmid n$, then $p\nmid n^2$
Since its contrapositive is always true, the statement is always true

c. Let p be a prime number, then $\sqrt{p}$ is irrational
Proof by contradiction:
Assume opposite is true, so if p is prime, then $\sqrt{p}$ is rational. A rational number must be equal to some integer a divided by an integer b, so $\sqrt{p} = \frac{a}{b}$
so $p = \frac{a^2}{b^2} \rightarrow pb^2 = a^2$, this statement shows that p divides a^2, and as we proved in part b, p must also divide a.
$\rightarrow$ so $a = pk$ where k is an integer
Substitute $pb^2 = (pk)^2 \rightarrow pb^2 = p^2k^2 \rightarrow b^2 = pk^2$
therefore p divides b^2 and likewise b. This results in a contradiction since they should be prime.
Therefore, if p is prime, $\sqrt{p}$ is irrational

3) prove or disprove that $p_1 p_2 \cdots p_n + 1$ is prime
for every positive integer n, $p_1, p_2, \ldots, p_n$ are
the smallest prime numbers.

So let $k = (p_1 p_2 \cdots p_n) + 1$, which makes k one
greater than each product of prime, making k a non-prime excep
$n = 1$. So we want to see if some prime number m can' divide k.
So let a be some integer and let m be
some prime number that divides k (so $m = p_1$

So we get $k = ma$, since we know
what k equals, we substitute.

$(p_1 p_2 \cdots p_n) + 1 = p_1 a$ ...
we know p_1 must be positive, which follows that a must
be positive because $p_1 \cdot a$ is positive, then subtract
and simplify so we have:
we have $1 = p_1 (a - (p_2 \cdots p_n))$

since we know $(a - (p_2 \cdots p_n))$ results
in a positive integer and p_1 is a prime
number greater than 1, we know the
product of $p_1 \cdot (a - (p_2 \cdots p_n))$ will
be greater than one, which contradicts
$1 = p_1 (a - p_2 \cdots p_n)$

4) a. $a \equiv 43 \bmod 23$ and $-22 \leq a \leq 0$

find integer a so $43 = 23q + r$ r is remainder and result

$a \equiv r$, when $q = 2$, $43 = 46 + r \rightarrow r = -3 = a$

b. $a \equiv 24 \bmod 31$ and $-15 \leq a \leq 15$, find integer a

so $24 = 31q + r$ $a \equiv r$

when $q = 1$, $24 = 31 + r \rightarrow r = -7 = a$

c. $a \equiv -15 \bmod 27$ and $-26 \leq a \leq 0$, find integer a

so $-15 = 27q + r$ $a \equiv r$

when $q = 0$ $-15 = r \equiv a$

d. $a \equiv -11 \bmod 21$ and $90 \leq a \leq 110$, find integer a

so $-11 = 21q + r$ $a \equiv r$

when $q = -5$, $-11 = 21(-5) + r \rightarrow -11 = -105 + r \rightarrow r = 94$

5) a. if $ac \equiv bc \bmod m$, a b c m are integers, $m \geq 2$, then $a \equiv b \bmod m$

$bc \bmod m \rightarrow bc = mq + r$, $r = ac$

$b \bmod m \rightarrow b = mq + k$, $k = a$

−2

$bc = mq + r \rightarrow bc = mq + ac \rightarrow b = \frac{mq}{c} + a$

$b = mq + k \rightarrow b = mq + a$ $\frac{mq}{c} + a = mq + a \longrightarrow$

$\frac{mq}{c} = mq \rightarrow \frac{1}{c} = 1 \rightarrow c = 1$

Note: In any case where $c \neq 1$, this statement will fail

~~b. if $a \equiv b \bmod m$ and $c \equiv d \bmod m$ where $a, b, c, d, m \in \mathbb{Z}$ with c and d positive, $m \geq 2$, $a^c \equiv b^d \bmod m$~~

~~$b = mq + r$ and $d = mq + k$ then $b^d = mq + L$~~

~~$(mq + a)^{mq + c} = mq + a^c$~~

~~$mq^{mq} + mq^c + a^{mq} + a^c = mq + a^c$~~

?

↑

take this work for

can select some random numbers and disprove it

6) a. if $2^p - 1$ is prime, then p is prime

proof by contraposition: if p is composite, then $2^p - 1$ is composite

let a, b be positive integers. Then we have $2^{ab} - 1$. Here we can expand the following:

$$2^{ab} - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + 2^{a(b-3)} + \dots 2^a + 1)$$

so if p is composite represented by ab, we know $2^{ab} - 1$ to be composite because it can be divided by $(2^a - 1)$. Thus because the contrapositive is true, the original statement must also be true.

b. if $a^n - 1$ is a prime number, then $a = 2$ and n is prime number.

again let $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \dots + x + 1)$

if $x^n - 1$ is prime then it must result that one of its factors is itself and the other factor is 1. so we can let $x - 1 = 1$, which results that $x = 2$ $(a = 2)$, we cant assume the other equals one because we assume x^{n-1} is prime which means its > 1, and because we know $x^n - 1 > 1$ and we add $+1$ at the end we know $(x^{n-1} + x^{n-2} + \dots + x + 1) > 1$. now we show that n must be prime because in part a we found when n is composite $2^n - 1$ was also composite, which proves the contraposition true, which makes the originally true.

7.) Find all positive integers m so the following are true:

−0.5

a. $13 \equiv 5 \bmod m$

so $5 = mq + r$ and $r = 13$

$\rightarrow 5 = mq + 13 \rightarrow mq = -8 \rightarrow m = -\frac{8}{q}$

for m to be a positive integer, $-\frac{8}{q}$ must evaluate to a whole positive number

when $q = -8, -4, -2,$ and -1, m results in the positive integers: $m = 1, 2, 4, 8$ respectively

$\boxed{\text{all positive integers}}$

b. $10 \equiv 1 \bmod m$

so $1 = mq + r$ and $r = 10$

$\rightarrow 1 = mq + 10 \rightarrow mq = -9 \rightarrow m = -\frac{9}{q}$

for m to be positive integer, $-\frac{9}{q}$ must evaluate to a whole positive number

when $q = -9, -3,$ and -1, m results in the positive integers: $m = 1, 3, 9$ respectively

c. $-7 \equiv 6 \bmod m$

so $6 = mq + r$ and $r = -7$

$6 = mq - 7 \rightarrow mq = 13 \rightarrow m = \frac{13}{q}$

for m to be a positive integer, $\frac{13}{q}$ must evaluate to a whole positive number

when $q = 13$ and 1, m results in the positive integers: $m = 1, 13$ respectively

d. $100 \equiv -5 \bmod m$

so $-5 = mq + r$ and $r = 100$

$\rightarrow -5 = mq + 100 \rightarrow mq = -105 \rightarrow m = -\frac{105}{q}$

for m to be a positive integer, $-\frac{105}{q}$ must evaluate to a whole positive number

when $q = -105, -35, -21, -15, -7, -5, -3,$ and -1, m results in positive integers: $m = 1, 3, 5, 7, 15, 21, 35, 105$ respectively