Math 445 HW #1 Solutions

1. Compute $(1819, 3587)$:

$$\begin{aligned}
3587 &= 1\cdot 1819 + 1768\\
1819 &= 1\cdot 1768 + 51\\
1768 &= 34\cdot 51 + 34\\
51 &= 1\cdot 34 + 17\\
34 &= 2\cdot 17 + 0
\end{aligned}$$

So $(1819, 3587) = (1768, 1819) = \cdots = (17, 0) = 17$, and

$$\begin{aligned}
17 &= 51 - 1\cdot 34 = 51 - 1\cdot(1768 - 34\cdot 51) = 35\cdot 51 - 1\cdot 1768\\
&= 35(1819 - 1\cdot 1768) - 1\cdot 1768 = 35\cdot 1819 - 36\cdot 1768\\
&= 35\cdot 1819 - 36(3587 - 1\cdot 1819) = 71\cdot 1819 + (-36)\cdot 3587
\end{aligned}$$

[Check: $71\cdot 1819 - 36\cdot 3587 = 129149 - 129132 = 17$ ✓
$1819 = 17\cdot 107$, $3587 = 17\cdot 211$]

2. For any n, $6 \mid n(n+1)(n+2)$ and $24 \mid n(n+1)(n+2)(n+3)$.

For any n, $n \equiv_6 0, 1, 2, 3, 4,$ or 5. If

$n \equiv_6 0$, then $6 \mid n$ so $6 \mid n(n+1)(n+2) = P_3(n)$

$n \equiv_6 1$, then $n+1 \equiv_6 2$ so $2 \mid n+1$, and $n+2 \equiv_6 3$ so $3 \mid n+2$, so
$2\cdot 3 \mid (n+1)(n+2)$, so $6 \mid P_3(n)$

$n \equiv_6 2$, then $n+1 \equiv_6 3$, so $2 \mid n$ and $3 \mid n+1$ so $6 \mid n(n+1) \mid P_3(n)$, so
$6 \mid P_3(n)$

$n \equiv_6 3$ then $n+1 \equiv_6 4$ so $3 \mid n$ and $2 \mid (n+1)$, so $6 \mid P_3(n)$ as above.

$n \underset{6}{\equiv} 4$, then ~~2~~ $n+2 \underset{6}{\equiv} 0$ so $6 \mid n+2$ so $6 \mid P_3(n)$

$n \underset{6}{\equiv} 5$, then $n+1 \underset{6}{\equiv} 0$ so $6 \mid n+1$ so $6 \mid P_3(n)$.

So no matter what value n has mod 6, $6 \mid P_3(n) = n(n+1)(n+2)$.

—

$P_4(n) = n(n+1)(n+2)(n+3) = P_3(n) \cdot (n+3)$

Since $6 \mid P_3(n)$, $3 \mid P_3(n)$, so $3 \mid P_4(n)$.

By looking at n mod 8 (or better, mod 4), we can conclude that one of $n, n+1, n+2, n+3$ is always $\underset{4}{\equiv} 2$, while another is $\underset{4}{\equiv} 0$ so $2 \mid$ one of them ~~and~~ $4 \mid$ another, so $8 \mid P_4(n)$ for every n.

Since $3 \mid P_4(n)$ and $8 \mid P_4(n)$ and $(3,8)=1$, $3 \cdot 8 = 24 \mid P_4(n)$.

General conjecture: For any n, k $k! \mid n(n+1)\cdots(n+k-1)$ [which is true!]

3. If p is prime and $p \underset{3}{\equiv} 1$, then $p \underset{6}{\equiv} 1$.

~~If $p \underset{6}{\equiv} a$ $a = 0, \ldots, 5$ then $p = 6x + a$ some integer x~~

~~So $p = 3(2x) + a$.~~

$p \underset{3}{\equiv} 1$ so $p = 3x+1$ some integer x.

x is either even or odd; if x is odd $x = 2n+1$, then $p = 3(2n+1)+1 = 6n+4 = 2(3n+2)$ is even (and ≥ 4) so cannot be prime. Therefore, x must be even $x = 2m$, so

$p = 3(2m)+1 = 6m+1$, so $p \underset{6}{\equiv} 1$.

4. If $x, y, z \in \mathbb{Z}$ and $x^2+y^2=z^2$, then $3|x$ or $3|y$.

Suppose not. Suppose $3 \nmid x$ and $3 \nmid y$. Then

$x = 3x' + a$, $a = 1$ or 2 and $y = 3y' + b$, $b = 1$ or 2

But then $x^2 = (3x'+a)^2 = 9(x')^2 + 6x'a + a^2 = 3(3(x')^2 + 2x'a) + a^2 \equiv_3 a^2$

$\equiv_3 1$ since $1^2 = 1 \equiv_3 1$ and $2^2 = 4 \equiv_3 1$.

Similarly, $y^2 \equiv_3 1$. So $x^2+y^2 \equiv_3 1+1 = 2$. So $z^2 \equiv_3 2$.

But that is impossible, since $z \equiv_3 0, 1,$ or 2 so

$z^2 \equiv_3 0^2 = 1$ or $1^2 = 1$ or $2^2 = 4 \equiv_3 1$, so $z^2 \equiv_3 0$ or 1.

So our assumption is false; so we must have either

$3|x$ or $3|y$.

The more general conjecture: $\forall n, \forall a \quad n! \mid a(a+1)\cdots(a+n-1)$

Proof by induction:

$n=1 \quad 1! \mid a$ for all a ✓ $1!=1$.

Suppose true for $n-1$, show true for n.

Show $n! \mid a(a+1)\cdots(a+n-1) \quad \forall a \geq 1$. By induction!

$a=1$: $n! \mid 1\cdot 2 \cdots (1+n-1) = n!$ ✓

Suppose true for a, show true for $a+1$.

We know $n! \mid a(a+1)\cdots(a+n-1)$

We want $n! \mid (a+1)\cdots(a+n-1)(a+n)$

But $(a+1)\cdots(a+n) = (a+1)\cdots(a+n-1)a + (a+1)\cdots(a+n-1)n$

$= a(a+1)\cdots(a+n-1) + (a+1)\cdots((a+1)+(n-1)-1)n$

By inductive hypoth., $n! \mid a(a+1)\cdots(a+n-1)$

By other inductive hypoth, $(n-1)! \mid (a+1)\cdots((a+1)+(n-1)-1)$

So $n! \mid n(a+1)\cdots((a+1)+(n-1)-1)$

So $n! \mid$ their sum, i.e. $n! \mid (a+1)\cdots((a+1)+n-1)$

So by induction $n! \mid a\cdots(a+n-1)$ for all $a \geq 1$.

So by induction, $\forall n \geq 1$, $n! \mid a\cdots(a+n-1)$ for all $a \geq 1$.