Math 310 Exam 1 practice problems solutions.

1. $5 \mid 3(7^n) + 17(2^n)$ all $n \geq 0$: $n=0$: $3 \cdot 7^0 + 17 \cdot 2^0 = 20 = 5 \cdot 4$ ✓

If $3(7^n) + 17(2^n) = 5k$, then $3(7^{n+1}) + 17(2^{n+1}) =$
$= 7(3 \cdot 7^n) + 2(17 \cdot 2^n) = 2(3 \cdot 7^n + 17 \cdot 2^n) + 5(3 \cdot 7^n)$
$= 2(5k) + 5(3 \cdot 7^n) = 5(2k + 3 \cdot 7^n)$. So
$5 \mid 3(7^n) + 17(2^n)$, then $5 \mid 3 \cdot (7^{n+1}) + 17(2^{n+1})$. So by induction, $5 \mid 3(7^n) + 17(2^n)$ for all $n \geq 0$.

2. $(432, 831)$:

$$831 = 432 \cdot 1 + 399$$
$$432 = 399 \cdot 1 + 33$$
$$399 = 33 \cdot 12 + 3$$
$$33 = 3 \cdot 11 + 0$$

So $(831, 432) = 3$

$$3 = 399 - 33 \cdot 12$$
$$= 399 - (432 - 399) \cdot 12$$
$$= 399 \cdot 13 - 432 \cdot 12$$
$$= (831 - 432) \cdot 13 - 432 \cdot 12$$
$$= 831 \cdot 13 - 432 \cdot 25$$
$$= 831 \cdot 13 + 432 \cdot (-25).$$

3. $3x^2 - y^3 = 176$ has no solutions. In $\mathbb{Z}_9$

x	0	1	2	3	4	5	6	7	8
x^2	0	1	4	0	7	7	0	4	1
x^3	0	1	8	0	1	8	0	1	8
$3x^2$	0	3	3	0	3	3	0	3	3

So $3x^2 = 0$ or 3 $y^3 = 0, 1$ or 8, so $3x^2 - y^3 = 0-0, 0-1, 0-8,$
$3-0, 3-1,$ or $3-8$

i.e. $3x^2 - y^3 = 0, -1 = 8, -8 = 1, 3, 2,$ or $3 - 8 = -5 = 4$.
$= 0, 1, 2, 3, 4,$ or $\underline{8}$, in $\mathbb{Z}_9$

But since $176 = 9 \cdot 19 + 5 \underset{9}{\equiv} 5$, we can't have $3x^2 - y^3 = 176$ in $\mathbb{Z}_9$, so $3x^2 - y^3 = 176$ has no solutions with $x, y \in \mathbb{Z}$.

4. n odd $(n \equiv_2 1)$ then $(n, n+8) = 1$ Oh, right, read the hint!

$(n, n+8)$ is the largest integer dividing both n and $n+8$

But if $d | n$ and $d | n+8$, then $d | (n+8)-n = 8$, so $d = 1, 2, 4,$ or 8.

But! n is odd, so $d | n \implies d$ is odd, so $d = 1$. So $(n, n+8) = 1$.

5. $a^2 \equiv_{10} 16$ implies $a^2 \equiv_{20} 16$.

$10 | a^2 - 16 = (a+4)(a-4)$. So $5 | (a+4)(a-4)$ so $5 |$ one of them.

Also, $2 | (a+4)(a-4)$ so $2 | a+4$ or $2 | a-4$. But since $2|4$ and $2|-4$ whichever of $a+4, a-4$ 2 divides, it then divides a so $a = 2k$ so $a^2 - 16 = (2k)^2 - 16 = 4(k^2 - 4)$ so $4 | a^2 - 16$. But then since $4 | a^2 - 16$ and $5 | a^2 - 16$, and $(4,5) = 1$, we know that $4 \cdot 5 | a^2 - 16$, so $a^2 \equiv 16 \pmod{20}$.

6. $(217, 133)$:

$$\begin{aligned}
217 &= 133 \cdot 1 + 84 \\
133 &= 84 \cdot 1 + 49 \\
84 &= 49 \cdot 1 + 35 \\
49 &= 35 \cdot 1 + 14 \\
35 &= 14 \cdot 2 + 7 \\
14 &= 7 \cdot 2 + 0
\end{aligned}$$

So $(217, 133) = 7$

$$\begin{aligned}
7 &= 35 - 14 \cdot 2 \\
&= 35 - (49 - 35) \cdot 2 \\
&= 35 \cdot 3 - 49 \cdot 2 \\
&= (84 - 49) \cdot 3 - 49 \cdot 2 \\
&= 84 \cdot 3 - 49 \cdot 5 \\
&= 84 \cdot 3 - (133 - 84) \cdot 5 \\
&= 84 \cdot 8 - 133 \cdot 5 \\
&= (217 - 133) \cdot 8 - 133 \cdot 5 \\
&= 217 \cdot 8 - 133 \cdot 13
\end{aligned}$$

$7 = 133 \cdot (-13) + 217 \cdot 8$

7. $3^{116} \pmod{29}$ $3^1 = 3$, $3^2 = 9$, $3^3 = 27$, $3^4 = 81 \equiv_{29} 23$, $3^5 \equiv_{29} 69 \equiv_{29} 11$, $3^6 \equiv_{29} 33 \equiv_{29} 4$, $3^7 \equiv_{29} 12$, $3^8 \equiv_{29} 36 \equiv_{29} 7$, $3^9 \equiv_{29} 21$, $3^{10} \equiv_{29} 63 \equiv_{29} 5$, $3^{11} \equiv_{29} 15$, $3^{12} \equiv_{29} 45 \equiv_{29} 16$, $3^{13} \equiv_{29} 48 \equiv_{29} 19$, $3^{14} \equiv_{29} 57 \equiv_{29} 28 \equiv_{29} (-1)$. So $(3^{14})^2 = 3^{28} \equiv_{29} (-1)^2 = 1$. So, since $116 = 28 \cdot 4 + 4$,

$3^{116} = (3^{28})^4 \cdot 3^4 \underset{29}{\equiv} 1^4 \cdot 3^4 \underset{29}{\equiv} 3^4 \underset{29}{\equiv} 23$. So $3^{116} \equiv 23 \pmod{29}$. //

8. p prime $a \in \mathbb{Z}_p$ and $a^2 = a$. Then $p \mid a^2 - a = a(a-1)$. So since p is prime, either $p \mid a$ (so $[a]_p = [0]_p$ in $\mathbb{Z}_p$) or $p \mid a-1$ (so $[a]_p = [1]_p$ in $\mathbb{Z}_p$).

This isn't true if n isn't prime. We want $n \mid a(a-1)$, so set $n = a(a-1)$ for, say $a = 4$, so $n = 12$. But then in $\mathbb{Z}_{12}$, $[4]_{12}^2 = [16]_{12} = [4]_{12}$, but $[4]_{12} \neq [0]_{12}$, and $[4]_{12} \neq [1]_{12}$.

9. $3 \mid 2^{2n+1} + 1$ for all $n \geq 0$.

$n=0$: $2^{2\cdot 0+1} + 1 = 2^1 + 1 = 3 = 3 \cdot 1$, so $3 \mid 2^{2\cdot 0+1} + 1$. ✓

If $2^{2n+1} + 1 = 3k$, then $2^{2(n+1)+1} + 1 = 2^{2n+3} + 1 = 2^{2n+1} 2^2 + 1$
$= 4(2^{2n+1}) + 1 = 4(2^{2n+1} + 1) - 4 + 1 = 4(3k) - 3 = 3(4k-1)$, so
$3 \mid 2^{2(n+1)+1} + 1$. So by induction, $3 \mid 2^{2n+1} + 1$ for all $n \geq 0$.

10. $\sqrt{15}$ is irrational.

Short way: If $\sqrt{15} = x/y$, $x, y \in \mathbb{Z}$, then $x^2 = 15 \cdot y^2$. But if we write $x = 2^{\alpha_2} \cdot 3^{\alpha_3} \cdots p_k^{\alpha_{p_k}}$, $y = 2^{\beta_2} \cdot 3^{\beta_3} \cdots p_\ell^{\beta_\ell}$ (prime factorizations), then

$$x^2 = 2^{2\alpha_2} \cdot 3^{2\alpha_3} \cdot 5^{2\alpha_5} \cdots p_k^{2\alpha_k} = 15 y^2 = 3 \cdot 5 \cdot y^2 = 2^{2\beta_2} \cdot 3^{2\beta_3+1} \cdot 5^{2\beta_5+1} \cdots p_\ell^{2\beta_\ell}$$

But since prime factorizations are unique, we have $k = \ell$ and, more importantly, $2\alpha_3 = 2\beta_3 + 1$ (and $2\alpha_5 = 2\beta_5 + 1$). But one is even and one is odd, a contradiction. So $\sqrt{15}$ can't be rational.

Longer way: If $\sqrt{15} = x/y$ then $x^2 = 15y^2$, so since $3 \mid 15y^2$,
assume $x,y > 0$.
$3 \mid x^2$, so since 3 is prime, $3 \mid x$, so $x = 3x_1$; then
$15y^2 = x^2 = (3x_1)^2 = 9x_1^2$ so $5y^2 = 3x_1^2$. So $3 \mid 5y^2$, so since $(3,5)=1$,
$3 \mid y^2$, so again $3 \mid y$. So $y = 3y_1$. So $5y^2 = 5(3y_1)^2 = 45y_1^2 = 3x_1^2$, so
$15y_1^2 = x_1^2$, so $\sqrt{15} = x_1/y_1$ with $x = 3x_1 > x_1$ (since $x_1 > 0$). Then
then set $\{x \in \mathbb{Z}, x > 0$ such that $\sqrt{15} = x/y$ for some $y \in \mathbb{Z}\}$ is
a set of natural numbers with no smallest element, contradicting
well-orderedness. So we can't write $\sqrt{15} = x/y$ with $x,y \in \mathbb{Z}$.
So $\sqrt{15}$ isn't rational. //

11. Smallest in $A = \{10u + 15v \in \mathbb{N} : u,v \in \mathbb{Z}\} \subseteq \mathbb{N}$ is the gcd of 10 & 15:

$$15 = 10 \cdot 1 + 5$$
$$10 = 5 \cdot 2 + 0$$

so $(10,15) = 5$, so smallest element of A is $\underline{\underline{5}}$.

12. $a,b,c \in \mathbb{Z}$ with $a \mid b$ and $a \mid b+c$, then $a \mid c$.

$a \mid b$ means $b = ax$; $a \mid b+c$ means $b+c = ay$; then
$c = (b+c) - b = ay - ax = a(y-x)$, so $a \mid c$. //

13. $127 \cdot 244 \cdot 14 \cdot (-45) \pmod{13}$:

$127 = 13 \cdot 9 + 10 \underset{13}{\equiv} 10$, $244 = 13 \cdot 18 + 10 \underset{13}{\equiv} 10$, $14 \underset{13}{\equiv} 1$,
$-45 = 13 \cdot (-4) + 7 \underset{13}{\equiv} 7$, so

$100 = 13\cdot 7 + 9$ $\qquad 63 = 13\cdot 4 + 11$

$$127\cdot 244\cdot 14\cdot(-45) \equiv_{13} 10\cdot 10\cdot 1\cdot 7 = 100\cdot 7 \equiv_{13} 9\cdot 7 = 63 \equiv_{13} 11.$$

So $127\cdot 244\cdot 14\cdot(-45)$ has remainder 11 on division by 13.

14. p prime and $p \mid a^2$ then $p \mid a$.

Since p is prime and $p \mid a^2 = a\cdot a$ we know that <u>either</u> $p \mid a$ or $p \mid a$, which means $p \mid a$!

15. If $[a]_n = [1]_n$ in $\mathbb{Z}_n$, then $(a,n) = 1$.

$[a] = [1]$ means a and 1 leave the same remainder when you divide by n, ie. a has remainder 1 when you divide by n. So $a = nx + 1$, so $1 = a\cdot 1 + n\cdot(-x)$. So 1 can be written as a combination of a and n. So 1 is the <u>smallest</u> natural number that can be expressed as a combination of a and n, so $1 = (a,n)$. ◢

<u>OR</u>

Same proof, through $1 = a\cdot 1 + n(-x)$. Then say: if $d \mid a$ and $d \mid b$, then $d \mid a\cdot 1 + n(-x) = 1$ so $d \mid 1$, so $d \le 1$. So the <u>greatest</u> common divisor of a and n is 1, ie., $(a,n) = 1$. ◢