Math 445 Exam 1 Solutions

1. Show that $3|n^3+5n$ for every $n \geq 1$.

Solution # 1: By induction. $f(n) = n^3 + 5n$; then $f(0) = 0^3 + 5 \cdot 0 = 0 = 3 \cdot 0$. If $f(n) = 3K$, then $f(n+1) = (n+1)^3 + 5(n+1) = n^3 + 3n^2 + 3n + 1 + 5n + 5 = (n^3+5n) + 3n^2 + 3n + 6 = f(n) + 3(n^2+n+2) = 3(K+n^2+n+2)$ is also a multiple of 3. So by induction, $3|f(n)$ for all $n \geq 0$.

Solution # 2: For every n, $n \equiv 0$ or $n \equiv 1$ or $n \equiv 2$, mod 3. But $n \equiv 0$ implies $n^3 \equiv 0^3 \equiv 0$, so $n^3 + 5n \equiv 0 + 5 \cdot 0 = 0$, so $3|n^3+5n$. $n \equiv 1$ implies $n^3 \equiv 1^3 \equiv 1$, so $n^3 + 5n \equiv 1 + 5 \cdot 1 = 6 \equiv 0$, so $3|n^3+5n$. $n \equiv 2$ implies $n^3 \equiv 2^3 = 8 \equiv 2$, so $n^3 + 5n \equiv 2 + 5 \cdot 2 = 12 \equiv 0$, so $3|n^3+5n$. So in all cases, $3|n^3+5n$.

Solution # 3: By Fermat's Little Theorem, since 3 is prime, for every n, $n^3 \equiv n \pmod 3$. So $n^3 + 5n \equiv n + 5n = 6n \equiv 0$, since $6 \equiv 0 \pmod 3$.

...and I saw at least two more essentially different solutions in your exams.

2. Use the facts that $\text{ord}_{23}(2) = 11$ and $\text{ord}_{23}(5) = 22$

to find the period of the repeating decimal expansion of $\dfrac{1}{23}$.

We wish to compute $\text{ord}_{23}(10)$. Since 23 is prime $10^{22} \equiv 1 \pmod{23}$ by Fermat's little theorem. So $\text{ord}_{23}(10)|22 = 2 \cdot 11$, so $\text{ord}_{23}(10) =$ 1,2,11, or 22. But $10 \not\equiv 1 \pmod{22}$, and $10^2 = 100 = 23 \cdot 4 + 8 \equiv 8 \not\equiv 1 \pmod{23}$, so it must be 11 or 22. But since $\text{ord}_{23}(5) = 22$, $5^{11} \not\equiv 1 \pmod{23}$, so $10^{11} = (2 \cdot 5)^{11} = 2^{11}5^{11} \equiv 1 \cdot 5^{11} = 5^{11} \not\equiv 1 \pmod{23}$, so $\text{ord}_{23}(10) \neq 11$. So the only remaining possibility must be true; $\text{ord}_{23}(10) = 22$. So the period of the repeating decimal expansion of $\dfrac{1}{23}$ is 22.

3. Show that if p is prime, $(a,p) = (b,p) = 1$, and *neither* of the equations

$$x^2 \equiv a \pmod p \qquad \text{or} \qquad x^2 \equiv b \pmod p$$

have a solution, then the equation $x^2 \equiv ab \pmod p$ *does* have a solution.

Since $x^2 \equiv a \pmod p$ and $x^2 \equiv b \pmod p$ each have no solution, by Euler's criterion $y = a^{\frac{p-1}{2}} \not\equiv 1 \pmod p$ and $z = b^{\frac{p-1}{2}} \not\equiv 1 \pmod p$. But since $y^2 = a^{p-1} \equiv 1$ and $z^2 = b^{p-1} \equiv 1$ and p is prime, we must have $y, z \equiv \pm 1$, so $y \equiv -1 \equiv z$, mod p . So $1 \equiv yz = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} = (ab)^{\frac{p-1}{2}}$, mod p, so by Euler's criterion, $x^2 \equiv ab \pmod p$ *does* have a solution.

4. For each of the following equations, determine if it has a solution, and if so, how many solutions (modulo 49):

(a): $x^5 \equiv 10 \pmod{49}$

$\Phi(49) = \Phi(7^2) = 7^1(7-1) = 42$, and $(5,42) = 1$, so by our result from class, $x^5 \equiv 10 \pmod{49}$ has a solution $\Leftrightarrow 10^{\frac{\Phi(49)}{(5,\Phi(49))}} = 10^{\frac{42}{1}} = 10^{42} \equiv 1 \pmod{49}$. But since $(10,49) = (2 \cdot 5, 7^2) = 1$, $10^{42} \equiv 1 \pmod{49}$ by Euler's Theorem. So $x^5 \equiv 10 \pmod{49}$ has $(5, \Phi(49) = 1$ solution.

(b): $x^7 \equiv 10 \pmod{49}$

As above, since $(7,42) = 7$, $x^7 \equiv 10 \pmod{49}$ has a solution $\Leftrightarrow 10^{\frac{\Phi(49)}{(7,\Phi(49))}} = 10^{\frac{42}{7}} = 10^6 \equiv 1 \pmod{49}$. But $10^2 = 100 = 49 \cdot 2 + 2 \equiv 2 \pmod{49}$, so $10^6 = (10^2)^3 \equiv 2^3 = 8 \not\equiv 1 \pmod{49}$. So $x^7 \equiv 10 \pmod{49}$ has no solutions.