Solutions for the Midterm for Math 301A–Spring, 2018

QUESTION 1. Suppose that $a \in \mathbf{Z}$ and that $a \equiv -23 \pmod{17}$.

(a) Find the remainder that a gives when divided by 17.

Solution: Notice that $-23 \equiv -23 + 2 \cdot 17 \pmod{17}$. That is, $-23 \equiv 11 \pmod{17}$. Therefore, we have $a \equiv 11 \pmod{17}$. Since $0 \leq 11 < 17$, it follows that a gives a remainder of 11 when divided by 17. We are using Congruence Proposition 11.

(b) What can you say (if anything) about the remainder that a gives when divided by 51?

Solution: First of all, if r denotes the remainder that a gives when divided by 51. then

$$a \equiv r \pmod{51} \qquad \textit{and} \qquad 0 \leq r < 51 \ .$$

Notice that $17 \big| 51$. It follows that $a \equiv r \pmod{17}$. We are using Congruence Proposition 9 here. Since $a \equiv 11 \pmod{17}$, we must have $r \equiv 11 \pmod{17}$. We are using the symmetric and transitive properties. Using the fact that $r \equiv 11 \pmod{17}$ together with the inequality $0 \leq r < 51$, we find the following three possibilities for r: $r = 11,\ r = 28,\ r = 45$

QUESTION 2. Suppose that p is a prime. Suppose that $a \in \mathbf{Z}$ and that $a^2 \equiv 1 \pmod{p}$. Prove that either $a \equiv 1 \pmod{p}$ or that $a \equiv p - 1 \pmod{p}$.

Solution: Since $a^2 \equiv 1 \pmod{p}$, it follows that $p \big| (a^2 - 1)$. Therefore,

$$p \big| (a-1)(a+1) \ .$$

Thus p divides the product of two integers. Since p is a prime, we can use one of the versions of Euclid's Lemma to conclude that p divides one factor or the other. Thus, either $p \big| (a-1)$ or $p \big| (a+1)$. If $p \big| (a-1)$, then, by definition, it follows that $a \equiv 1 \pmod{p}$. On the other hand, if $p \big| (a+1)$, then we have $a \equiv -1 \pmod{p}$. Notice that $-1 \equiv -1 + p \pmod{p}$. That is, we have $-1 \equiv p - 1 \pmod{p}$. Thus, if $a \equiv -1 \pmod{p}$, then it follows that $a \equiv p - 1 \pmod{p}$. In summary, we have proved that either $a \equiv 1 \pmod{p}$ or $a \equiv p - 1 \pmod{p}$.

QUESTION 3. (20 points) Suppose that $e,\ f \in \mathbf{Z}$ and that $gcd(e, f) = 1$. TRUE OR FALSE: *There exist integers u and v such that $ue^4 + vf^4 = -1$.* Justify your answer carefully.

Solution: The statement is true. We will use divisibility proposition 14. We first want to point out that the assumption that $m \geq 1$ in that proposition is not needed. In fact, If $a, b \in \mathbf{Z}$, and not both are zero, then $gdc(a, b)$ is defined and is unchanged if one multiplies a and/or b by -1. This is so because the divisors of a and $-a$ are the same. The divisors of b and $-b$ are the same too. Thus, the set of common divisors of a and b is unchanged if one replaces a by $-a$ or b by $-b$.

Since $gcd(e, f) = 1$, divisibility proposition 14 implies that $gcd(e \cdot e \cdot e \cdot e, f) = 1$. That is, $gcd(e^4, f) = 1$. Thus, $gcd(f, e^4) = 1$. Using proposition 14 again (with $m = e^4$), it follows that $gcd(f \cdot f \cdot f \cdot f, e^4) = 1$. That is, $gcd(f^4, e^4) = 1$. We have therefore shown that $gcd(e^4, f^4) = 1$. By divisibility proposition 4, it follows that there exist integers m and n such that $me^4 + nf^4 = 1$. Letting $u = -m$ and $v = -n$, we then have $ue^4 + vf^4 = -1$ for that choice of integers u and v.

QUESTION 4. (20 points) Let $n = 5^{50} + 13^{17} + 3^{15}$. Prove that $65 \big| n$.

(Note that $65 = 5 \cdot 13$.)

Solution: First of all, note that $5 \big| 5^{50}$ and hence $5^{50} \equiv 0 \pmod{5}$. Secondly, notice that $13 \equiv 3 \pmod{5}$ and hence $13^{17} \equiv 3^{17} \pmod{5}$. We have used Congruence Property 6. We use that property later too. We have

$$13^{17} + 3^{15} \;\equiv\; 3^{17} + 3^{15} \;\equiv\; 3^{15}\big(3^2 + 1\big) \;\equiv\; 3^{15} \cdot 10 \;\equiv\; 3^{15} \cdot 0 \;\equiv\; 0 \pmod{5} \ .$$

We have used the fact that $10 \equiv 0 \pmod{5}$. It follows that

$$n = 5^{50} + \big(13^{17} + 3^{15}\big) \;\equiv\; 0 \;+\; 0 \;\equiv 0 \pmod{5} \ .$$

Now notice that $13 \big| 13^{17}$ and hence $13^{17} \equiv 0 \pmod{13}$. Also, notice that

$$5^2 = 25 \equiv -1 \pmod{13} \ .$$

Therefore,

$$5^{50} \;=\; (5^2)^{25} \;\equiv\; (-1)^{25} \;\equiv\; -1 \pmod{13} \ .$$

Furthermore, notice that $3^3 = 27 \equiv 1 \pmod{13}$. Therefore,

$$3^{15} \;=\; (3^3)^5 \;\equiv\; 1^5 \;\equiv 1 \pmod{13} \ .$$

It follows that

$$n = 5^{50} + 13^{17} + 3^{15} \;\equiv\; -1 \;+\; 0 \;+\; 1 \;\equiv\; 0 \pmod{13} \;\;.$$

We have shown that $n \equiv 0 \pmod 5$ and $n \equiv 0 \pmod{13}$. Since $gcd(5, 13) = 1$, it follows (by using Congruence Property 10) that $n \equiv 0 \pmod{5 \cdot 13}$. That is, $n \equiv 0 \pmod{65}$.

QUESTION 5. Suppose that $a \in \mathbf{Z}$ and that $a \geq -10$. Suppose also that $a \equiv 1 \pmod 7$. Carefully prove that $a + 20$ cannot be a prime.

Solution: Since $a \equiv 1 \pmod 7$ and $20 \equiv 20 \pmod 7$, it follows that

$$a + 20 \equiv 1 + 20 \pmod 7 \;\;.$$

Now $1 + 20 = 21 \equiv 0 \pmod 7$. Thus, we have $a + 20 \equiv 0 \pmod 7$. It follows that $a + 20$ is divisible by 7.

Furthermore, since $a \geq -10$, we have $a + 20 \geq 10$. Therefore, $a + 20 > 7$. In summary, we know $a + 20 = 7q$, where $q \in \mathbf{Z}$, and that $1 < 7 < a + 20$. It is clear that q is a positive integer since $a+20$ is positive. Since $7 < a+20$, it is clear that $q \neq 1$. Therefore $a+20 = 7q$ is a product of two positive integers 7 and q and neither factor is equal to 1. Hence, $a + 20$ cannot be a prime.