Homework 4

Walker Bagley

October 1, 2024

(1)

Prove that if a and b are integers and p is a prime, then $(a+b)^p \equiv a^p + b^p \pmod{p}$. You may assume that the binomial coefficient $\frac{p!}{r!(p-r)!}$ is an integer.

Proof.

$$\begin{aligned}(a+b)^p &= a^p + \frac{p!}{1!(p-1)!}a^{p-1}b + \frac{p!}{2!(p-2)!}a^{p-2}b^2 + \ldots + \frac{p!}{(p-2)!2!}a^2b^{p-2} + \frac{p!}{(p-1)!1!}ab^{p-1} + b^p \\ &= a^p + pa^{p-1}b + \frac{p(p-1)}{2}a^{p-2}b^2 + \ldots + \frac{p(p-1)}{2}a^2b^{p-2} + pab^{p-1} + b^p\end{aligned}$$

Since all the binomial coefficients are integers and p is prime, all but the first and last coefficients (which are equal to 1) are divisible by p. Then

$$a^p + pa^{p-1}b + \frac{p(p-1)}{2}a^{p-2}b^2 + \ldots + \frac{p(p-1)}{2}a^2b^{p-2} + pab^{p-1} + b^p \equiv a^p + b^p \pmod{p}$$

□

(5)

Is the following equality true? $9682903^{17} + 7103689^{17} = 9859172^{17}$? (There are many ways to do this, explain your own reasoning. You are welcome to use any known result, as long as you can explain why it is true.)

Proof. Checking the prime factors of 9682903 gives 59, 164117 so if this equation is true, it must hold modulo 59. Then we have

$$\begin{gathered}9682903^{17} + 7103689^{17} \equiv 9859172^{17} \pmod{59} \\ 0^{17} + 30^{17} \equiv 36^{17} \pmod{59} \\ 30 \cdot (30^2)^8 \equiv 36 \cdot (36^2)^8 \pmod{59} \\ 30 \cdot (15)^8 \equiv 36 \cdot (57)^8 \pmod{59} \\ 30 \cdot (15^2)^4 \equiv 36 \cdot (57^2)^4 \pmod{59} \\ 30 \cdot (48)^4 \equiv 36 \cdot (4)^4 \pmod{59} \\ 30 \cdot (48^2)^2 \equiv 36 \cdot 256 \pmod{59} \\ 30 \cdot (3)^2 \equiv 36 \cdot 20 \pmod{59} \\ 270 \equiv 720 \pmod{59} \\ 34 \equiv 12 \pmod{59}\end{gathered}$$

Clearly, $34 \not\equiv 12 \pmod{59}$, so this equality does not hold modulo 59 and thus the equality is false. □

(6)

Show that the equation $x^2 + y^2 + z^2 = 20152015$ has no integral solutions. [Hint: Try congruences modulo powers of 2.]

Proof.

$$\begin{cases} x^2 + y^2 + z^2 \pmod 2 \equiv 20152015 \equiv 1 & x = y = z = 1 \\ x^2 + y^2 + z^2 \pmod 4 \equiv 20152015 \equiv 3 & x = y = z = 1 \\ x^2 + y^2 + z^2 \pmod 8 \equiv 20152015 \equiv 7 & ??? \end{cases}$$

Considering quadratic residuals modulo 8, we see that

$$\begin{cases} 1^2 \pmod 8 \equiv 1 \\ 2^2 \pmod 8 \equiv 4 \\ 3^2 \pmod 8 \equiv 1 \\ 4^2 \pmod 8 \equiv 0 \\ 5^2 \pmod 8 \equiv 1 \\ 6^2 \pmod 8 \equiv 4 \\ 7^2 \pmod 8 \equiv 1 \end{cases}$$

Then x^2, y^2, z^2 must be equal to one of $0, 1, 4$ modulo 8 since $x^2 \pmod 8 = [x \pmod 8]^2$. Then if one or fewer of x^2, y^2, z^2 is equivalent to $4 \pmod 8$, $x^2 + y^2 + z^2 \leq 6 < 7$. If two of x^2, y^2, z^2 are equivalent to 4 $\pmod 8$, then $x^2 + y^2 + z^2$ is equivalent to the last quadratic residual, $0, 1, 4 \neq 7$. If all three are equivalent to $4 \pmod 8$, then $x^2 + y^2 + z^2 \equiv 4 \pmod 8 \not\equiv 7$.

So, it is impossible to find a solution to $x^2 + y^2 + z^2 = 20152015$ modulo 8, and we know that there must be a solution to the equation modulo 8 if there is a solution to the general form, so $x^2 + y^2 + z^2 = 20152015$ has no integral solutions. □

(9)

Let p be a prime and consider the rational number $\frac{m}{n} = 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{p-1}$. If $p > 2$ show that $p|m$.

Proof.

$$\begin{aligned} \frac{m}{n} &= 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{p-1} \\ &= \left(1 + \frac{1}{p-1}\right) + \left(\frac{1}{2} + \frac{1}{p-2}\right) + \ldots + \left(\frac{1}{\frac{p-1}{2}} + \frac{1}{\frac{p+1}{2}}\right) \\ &= \frac{p}{p-1} + \frac{p}{2(p-2)} + \ldots + \frac{p}{\left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right)} \end{aligned}$$

Then if we combine these terms, since none of the denominator terms are divisible by p, p will not divide n. However, the numerator will be a sum of p terms multiplied by the various denominators, so $p|m$. □

(10)

Let n be a number such that $n + 1$ is divisible by 24. If $d|n$ show that 24 divides $d^2 - 1$.

Proof. If $24|n + 1$ then we know that $24k = n + 1$ for some $k \in \mathbb{Z}$, thus $n = 24k - 1$ and so n is odd. Then if $d|n$ and n is odd, then d must be odd. So, $d - 1$ and $d + 1$ are both even, and since they are consecutive even numbers, one of them must be divisible by 4. Additionally, since $24|n + 1$, then $3|n + 1$, so $3 \nmid n$ and thus $3 \nmid d$ because if $3|d$ and $d|n$, then $3|n$. We know that with 3 consecutive numbers $d - 1, d, d + 1$, one must be divisible by 3 and since $3 \nmid d$, 3 divides either $d - 1$ or $d + 1$. Then we have between $d - 1$ and $d + 1$ divisors of $2, 3, 4$ which means that $2 \cdot 3 \cdot 4 = 24|(d - 1)(d + 1) = d^2 - 1$, so 24 divides $d^2 - 1$. □