Problem 1.

a) Compute $gcd(85, 289)$ using Euclid's extended algorithm.

Answer: gcd(85, 289) = 17

$$\begin{aligned} 289 &= 3 * 85 + 34 \\ 85 &= 2 * 34 + 17 \\ 34 &= 2 * 17 + 0 \\ gcd(85, 289) &= 17 \end{aligned}$$

b) Compute x and y such that $85x + 289y = gcd(85, 289)$. Show your work.

Answer: $x = 7$ and $y = -2$

$$\begin{aligned} 17 &= 85 + (-2) \times 34 \\ 34 &= 289 + (-3) \times 85 \end{aligned}$$

$$\begin{aligned} 17 &= 85 + (-2) \times (289 + (-3) \times 85) \\ 17 &= 85 + (-2) \times 289 + 6 \times 85 \\ 17 &= 7 \times 85 - 2 \times 289 \end{aligned}$$

To show this is correct, $7 \times 85 - 2 \times 289 = 595 - 578 = 17$.

Problem 2.

Use Fermat's little theorem to compute $3^{62}\ (mod\ 7)$. Show your work.

Answer: Since 7 is prime and 3 is not divisible by 7 the theorem implies that $3^6 \equiv 1\ (mod\ 7)$.

$$\begin{aligned} 3^{62}\ (mod\ 7) &= ((3^6)^{10} \times 3^2)\ (mod\ 7) \\ 3^{62}\ (mod\ 7) &= (1^{10} \times 9)\ (mod\ 7) \\ 3^{62}\ (mod\ 7) &= 9\ (mod\ 7) \\ 3^{62}\ (mod\ 7) &= 2 \end{aligned}$$

Problem 3.

a) Show that $n^7 - n$ is divisible by 42 for every positive integer n.

Answer: To prove this we need to show that $n^7 - n$ is divisible by the prime factors of 42 for all n. These factors are 2, 3, and 7.

From Fermat's Little Theorem $p|(n^p - n)$ for all n if p is prime. $p = 7$ and 7 is prime, thus $7|(n^7 - n)$ for all n.

Fermat's Little Theorem also then shows that $3|(n^3 - n)$. Factoring $n^7 - n$ we get,

$$n^7 - n = n(n-1)(n+1)(n^2+n+1)(n^2-n+1) = (n^3-n)(n^4+n^2+1)$$

Thus $3|(n^7 - n)$ for all n.

Regardless of the value of n, $n^7 - n$ will always be even, thus $2|(n^7 - n)$ for all n.

So $42|(n^7 - n)$ for all positive n.

b) Show that every prime not equal to 2 or 5 divides infinitely many of the numbers 1, 11, 111, 1111, etc.

Answer: For p that is not 2 or 5, we have $10^{p-1} \equiv 1 \pmod{p}$ by Fermat's little theorem. Doing some modular multiplicative arithmetics, we also have $10^{k(p-1)} \equiv 1 \pmod{p}$ for $k \in \mathbb{Z}$, meaning $p \mid 10^{k(p-1)} - 1$. $10^{k(p-1)} - 1$ ($k \in \mathbb{Z}$) is such sequence that each number is just $k(p-1)$ 9s. So it's now showed that every prime not equal to 2 or 5 divides infinitely many of the numbers 9, 99, 999, 9999, etc.

Also because for a prime $p > 5$, p will not divide 9. So if p does not divide 9 but divides infinitely many of the numbers 9, 99, 999, 9999, etc, it must divide infinitely many of the numbers 1, 11, 111, 1111, etc.

$p = 3$ is a special case since it divides 9. But it's known that 3 will also divide infinitely many of the numbers 1, 11, 111, 1111, etc, as long as the number of 1s consisting the number is divisible by 3. QED.

c) Show that if $p > 3$ is a prime, then $p^2 \equiv 1 \pmod{24}$.

Answer: This is equivalent to stating that $24|(p^2 - 1)$. So the factors of $p^2 - 1 = (p-1)(p+1)$. In any three consecutive numbers at least one is divisible by 3. Since $p > 3$ this means that either $3|(p-1)$ or $3|(p+1)$. Since p is prime it is also odd, so $p - 1$ and $p + 1$ are both even. Since they are consecutive one of them is divisible by 2 and the other is divisible by 4. So $p^2 - 1$ is divisible by $2 \times 3 \times 4 = 24$. And since $p^2 = (p^2 - 1) + 1$ we know that $p^2\ (mod\ 24) \equiv 1\ (mod\ 24)$.

Problem 4.

a) Prove that if p is prime, and $0 < k < p$, then $p|\binom{p}{k}$.

Answer:

$$p|\binom{p}{k} = \frac{p!}{k!(p-k)!}$$

p is prime and only divisible by 1 and p. Since $k < p$ and $(p-k) < p$ then all values in the denominator are $< p$. So p is never cancelled out. Since $\binom{p}{k}$ results in an integer and p is prime, this implies that p is a factor of $\binom{p}{k}$. Thus, if p is prime, and $0 < k < p$, then $p|\binom{p}{k}$.

b) Prove that for all integers a and b and all primes p,

$$(a+b)^p \equiv a^p + b^p \ (mod\ p)$$

Answer: Let p be prime. Then by the binomial theorem,

$$(a+b)^p = b^p + \binom{p}{1}b^{p-1}a + \binom{p}{2}b^{p-2}a^2 + ... + \binom{p}{p-k}ba^k + a^p$$

From problem 4a we know that if p is prime and $0 < k < p$ then $p|\binom{p}{k}$. Given this all the middle terms in the above equation disappear with $(mod\ p)$, leaving $(a+b)^p = a^p + b^p\ (mod\ p)$. Thus for all integers a and b and all primes p, $(a+b)^p \equiv a^p + b^p\ (mod\ p)$.

Problem 5.

Let a be 1 in the previous problem, and use its conclusion to prove Fermat's little theorem.

Answer: This can be proved by induction.

Prove: Fermat's Little Theorem, $b^p \equiv b\ (mod\ p)$.

Let p be prime. As our base case let $b = 1$, then $1^p \equiv 1\ (mod\ p) \to 1 \equiv 1\ (mod\ p)$, which true since any prime is greater than 1. It's also true for $b = 0$ since $0 \equiv 0\ (mod\ p)$, if we need to consider 0 as an integer. Assume this holds for some integer b, so $b^p \equiv b\ (mod\ p)$. Then for $b+1$, we want to prove,

$$(b+1)^p \equiv b+1\ (mod\ p).$$

Given the result of question 4b, we know that $(b+1)^p \equiv b^p + 1^p\ (mod\ p) = (b+1)^p \equiv b^p + 1\ (mod\ p)$. Since $b^p \equiv b\ (mod\ p)$ then $(b+1)^p \equiv b+1\ (mod\ p)$.

Having shown $b^p \equiv b\ (mod\ p)$ holds for $b = 1$, as well as if $b^p \equiv b\ (mod\ p)$, then $(b+1)^p \equiv b+1\ (mod\ p)$ for $b \geq 1$, $b^p \equiv b\ (mod\ p)$ holds for all integers b and primes p.