God made the integers, all else is the work of man. (Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk.). - Leopold Kronecker

Question 1. Prove that there are infinitely many primes of the form $4n-1$.

Solution:
First of all, notice that every natural number is either $0, 1, 2$ or $3 \mod 4$. No prime number can be 0 modulo 4 because it would be divisible by 4. Also, every $n \equiv 2 \mod 4$ is an even number (why?) so the only prime $p \equiv 2 \mod 4$ is $p = 2$. Thus, every odd prime is either $p \equiv 1$ or $3 \mod 4$. Suppose for a contradiction that there are only finitely many primes congruent to $3 \mod 4$ and call them $p_1, \dots, p_n$. Let us consider the number:

$$N = 4p_1p_2 \cdots p_n - 1.$$

Notice that $N \equiv -1 \equiv 3 \mod 4$. Therefore N is odd and not divisible by 2. By the Fundamental Theorem of Arithmetic, N has a prime factorization into primes:

$$N = 4p_1p_2 \cdots p_n - 1 = q_1q_2 \cdot q_r$$

for some (odd) primes $q_1, q_2, \dots, q_r$. Suppose that all q_i are $\equiv 1 \mod 4$. Then:

$$N = q_1q_2 \cdot q_r \equiv 1 \cdot 1 \cdots 1 \equiv 1 \mod 4$$

but we proved above that $N \equiv 3 \mod 4$. Therefore, it must be the case that at least one prime q_i, divisor of N, is $\equiv 3 \mod 4$. But then, q_i must be one of the primes $p_1, \dots, p_n$. Hence q_i divides N, and also divides $p_1p_2 \cdots p_n$, and hence, q_i divides $N - 4p_1p_2 \cdots p_n = -1$, but this is clearly impossible.

Hence we have reached a contradiction, and there cannot be just finitely many primes of the form $4n-1$ (i.e. $\equiv 3 \mod 4$).

Question 2. Prove that there are infinitely many primes of the form $6n-1$.

Solution:
First of all, notice that every natural number is either $0, 1, 2, 3, 4$ or $5 \mod 6$. No prime number can be 0 modulo 6 because it would be divisible by 6. Also, every $n \equiv 2 \mod 6$ is an even number (why?) so the only prime $p \equiv 2 \mod 6$ is $p = 2$, and every $n \equiv 3 \mod 6$ is a multiple of 3 (why?) so the only prime $p \equiv 3 \mod 6$ is $p = 3$. Thus, every prime > 3 is either $p \equiv 1$ or $5 \mod 6$. Suppose for a contradiction that there are only finitely many primes congruent to $5 \mod 6$ and call them $p_1, \dots, p_n$. Let us consider the number:

$$N = 6p_1p_2 \cdots p_n - 1.$$

Notice that $N \equiv -1 \equiv 5 \mod 6$. Therefore N is odd and not divisible by 2 or 3. By the Fundamental Theorem of Arithmetic, N has a prime factorization into primes:

$$N = 6p_1p_2 \cdots p_n - 1 = q_1q_2 \cdot q_r$$

for some (odd) primes $q_1, q_2, \dots, q_r$. Suppose that all q_i are $\equiv 1 \mod 6$. Then:

$$N = q_1q_2 \cdot q_r \equiv 1 \cdot 1 \cdots 1 \equiv 1 \mod 6$$

but we proved above that $N \equiv 5 \mod 6$. Therefore, it must be the case that at least one prime q_i, divisor of N, is $\equiv 5 \mod 6$. But then, q_i must be one of the primes $p_1, \ldots, p_n$. Hence q_i divides N, and also divides $p_1 p_2 \cdots p_n$, and hence, q_i divides $N - 6p_1p_2\cdots p_n = -1$, but this is clearly impossible.

Hence we have reached a contradiction, and there cannot be just finitely many primes of the form $6n-1$ (i.e. $\equiv 5 \mod 6$).

Question 3. Let $a_1 = 2$ and $a_{n+1} = a_n(a_n - 1) + 1$. Prove that $a_{n+1} = a_1 a_2 \cdots a_n + 1$. Prove that for all $m \neq n$, the numbers a_m and a_n are relatively prime.

Solution:
We prove the first equality by induction. First, we deal with the base case $n = 2$:

$$a_2 = a_1(a_1 - 1) + 1 = 2(2-1) + 1 = 2 \cdot 1 + 1 = 3 = a_1 + 1.$$

Now suppose that the equality $a_n = a_1 a_2 \cdots a_{n-1} + 1$ holds (or equivalently, $a_n - 1 = a_1 a_2 \cdots a_{n-1}$) , and we want to prove it for $n+1$. We see that:

$$a_{n+1} = a_n(a_n - 1) + 1 = a_n(a_1 a_2 \cdots a_{n-1}) + 1 = a_1 a_2 \cdots a_n + 1$$

as claimed. Thus, by the Principle of Mathematical Induction, the equality holds for all $n \geq 2$.

In order to prove that for all $m \neq n$, the numbers a_m and a_n are relatively prime, we shall prove that for all $n \geq 2$, a_n is relatively prime to all a_m with $1 \leq m < n$. Indeed, if d divides a_n and a_m then d also divides

$$a_n - a_1 a_2 \cdots a_{n-1} = 1$$

and therefore $d = \pm 1$. Hence, the GCD of a_m and a_n must be 1.

Question 4. Prove that for any $n \geq 1$ there are n consecutive composite numbers.

Solution:
Let $n \geq 1$ and consider the number $N = (n+1)! + 2$, and the n consecutive numbers

$$N, N+1, N+2, \ldots, N+(n-1).$$

Notice that $N = (n+1)! + 2$ is divisible by 2 (and larger than 2, so it must be composite), $N + 1 = (n+1)! + 3$ is divisible by 3 (and larger than 3), and $N + i = (n+1)! + 2 + i$ is divisible by $2 + i$, as long as $0 \leq i \leq n-1$.

Question 5. Prove that for any $n \geq 2$ there is a prime p with $n < p \leq n! + 1$.

Solution:
If $n!+1$ is prime, then pick $p = n!+1$. Otherwise, if $n!+1$ is composite, then it has a prime factor q with $1 < q < n! + 1$. If $n < q < n! + 1$ then pick $p = q$. Otherwise, if $1 < q \leq n$ then q divides $n! + 1$ but it also divides $n!$ and so q would divide 1. That's impossible, so we must have $n < q \leq n! + 1$ and we can pick $p = q$.

Question 6. Find the least non-negative residues.

(a) 365 mod 5.

(b) -3122 mod 3.

(c) 3122082546 mod 10.

(d) -2445678 mod 10.

Solution:
Show your work!

1. $365 \equiv 0 \mod 5$ because $365 = 5 \cdot 73 + 0$.
2. $-3122 \equiv 1 \mod 3$ because $-3122 = 3(-1041) + 1$.
3. $3122082546 \equiv 6 \mod 10$ because $3122082546 = 312208254 \cdot 10 + 6$.
4. $-2445678 \equiv -8 \equiv 2 \mod 10$ because $-2445678 = (-244568) \cdot 10 + 2$.

Question 7. Find one integer $a \in \mathbb{Z}$ that satisfies, simultaneously, both congruences $a \equiv 5 \mod 8$ and $a \equiv 3 \mod 7$.

Solution:
If $a \equiv 5 \mod 8$ then $a = 5 + 8x$ for some integer x. If $a \equiv 3 \mod 7$ then $5 + 8x = 3 + 7y$ for some integer y. Thus $8x - 7y = -2$. The equation $8x - 7y = 1$ has a solution $x = y = 1$. Thus $8x - 7y = -2$ has a solution $x = y = -2$. Thus $a = 5 + 8(-2) = 5 - 16 = -11$ works. (Check your work: $a = -11 \equiv -3 \equiv 5 \mod 8$ and $a = -11 \equiv -4 \equiv 3 \mod 7$, so it does work).

Question 8. Show that if $n > 4$ is not prime then $(n-1)! \equiv 0 \mod n$.

Solution:
Suppose n is composite. Then there are a, b with $n = ab$ and $1 < a, b < n$.

If $1 < a < b < n$ then:

$$(n-1)! = 1 \cdot 2 \cdot 3 \cdots a \cdots b \cdots (n-1)$$

so clearly $(n-1)!$ is divisible by $ab = n$ and it must be $\equiv 0 \mod n$.

If $a = b$, i.e. $n = a^2$, as long as $a > 1$ we have:

$$(n-1)! = 1 \cdot 2 \cdot 3 \cdots a \cdots 2a \cdots 3a \cdots (a-1)a \cdots (a^2 - 1)$$

where $a^2 - 1 = n - 1$. Thus, $(n-1)!$ is divisible by (at least) $a \cdot 2a = 2a^2$, and therefore n divides $(n-1)!$.

Question 9. Prove the following properties of congruences:

(a) If $a \equiv b \mod n$ then $ka \equiv kb \mod n$.

(b) If $a \equiv b \mod n$ and $a' \equiv b' \mod n$ then $a + a' \equiv b + b' \mod n$.

Solution:

1. Suppose $a \equiv b \mod n$. That means n divides $a-b$, i.e. there exists d such that $a-b=dn$. Thus, also, $ka-kb=kdn$ which means that n divides $ka-kb$, or equivalently $ka \equiv kb \mod n$.

2. Suppose $a \equiv b \mod n$ and $a' \equiv b' \mod n$. Then there are integers d and d' such that $a-b=dn$ and $a'-b'=d'n$. Thus:

$$a+a'-(b+b')=(a-b)+(a'-b')=dn+d'n=(d+d')n$$

and so, n divides $a+a'-(b+b')$ which means that $a+a' \equiv b+b' \mod n$.

Question 10. Use congruences to show that $6 \cdot 4^n \equiv 6 \mod 9$ for any $n \geq 0$.

Solution:
The powers of 4 modulo 9 are

$$4, 4^2 \equiv 16 \equiv 7, 4^3 \equiv 7 \cdot 4 \equiv 28 \equiv 1, 4^4 \equiv 4, \ldots$$

i.e.

$$4, 7, 1, 4, 7, 1, 4, 7, 1, \ldots$$

But $6 \cdot 4 \equiv 24 \equiv 6 \mod 9$, $6 \cdot 7 \equiv 42 \equiv 6 \mod 9$ and $6 \cdot 1 \equiv 6 \mod 9$. Therefore, $6 \cdot 4^n \equiv 6 \mod 9$ for all $n \geq 1$.

Another way: $6 \cdot 4^n \equiv 6 \mod 9$ if and only if $2 \cdot 4^n \equiv 2 \mod 3$. But this last congruence is obvious because $4 \equiv 1 \mod 3$ and then $4^n \equiv 1 \mod 3$ for all $n \geq 1$.

Question 11. Find the least nonnegative residues.
(a) 5^{18} mod 7.

(b) 68^{105} mod 13.

(c) 6^{47} mod 12.

Solution:

1. $5^{18} \equiv (-2)^{18} \equiv 2^{18} \mod 7$. Notice as well that $2^3 \equiv 8 \equiv 1 \mod 7$. Thus $2^{18} \equiv (2^3)^6 \equiv 1^6 \equiv 1 \mod 7$. Hence $5^{18} \equiv 1 \mod 7$.

2. $68^{105} \equiv 3^{105} \mod 13$. Notice that $3^3 \equiv 27 \equiv 1 \mod 13$. Thus, $3^{105} \equiv (3^3)^{35} \equiv 1^{35} \equiv 1 \mod 13$.

3. Notice that $6^2 \equiv 36 \equiv 0 \mod 12$. Thus $6^{47} \equiv 6^2 \cdot 6^{45} \equiv 0 \cdot 6^{45} \equiv 0 \mod 12$.

Question 12. Show that $5^e + 6^e \equiv 0 \mod 11$ for all odd numbers e.

Solution:
$5^e + 6^e \equiv 5^e + (-5)^e \equiv 5^e - 5^e \equiv 0 \mod 11$. Notice that $(-5)^e = -5^e$ because e is odd.

Question 13. Prove the part (a), then find the least nonnegative residue modulo 7, 11 and 13 in parts (b), (c) and (d).

(a) A number N is congruent modulo 7, 11, or 13, to the alternating sum of its digits in base 1000. (For example, $123456789 \equiv 789 - 456 + 123 \equiv 456 \bmod 7, 11$, or 13.)

(b) 11233456,

(c) 58473625,

(d) $100, 000, 000, 000, 000, 001$.

Solution:

1. Let us write N in base 1000, as follows:

$$N = a_n \cdot 1000^n + a_{n-1} \cdot 1000^{n-1} + \cdots + a_2 \cdot 1000^2 + a_1 \cdot 1000 + a_0,$$

where each digit $0 \leq a_i \leq 999$. Note that $1000 = 1001 - 1 = 7 \cdot 11 \cdot 13 - 1$. Therefore, $1000 \equiv -1 \bmod 7$, 11 and 13. Hence,

$$N \equiv a_n(-1)^n + a_{n-1} \cdot (-1)^{n-1} + \cdot + a_2(-1)^2 + a_1(-1) + a_0 \bmod 7,\ 11,\ \text{ or }\ 13.$$

2. $11233456 \equiv 11 - 233 + 456 \equiv 234 \mod 7, 11$ or 13. And $234 \equiv 3 \mod 7$, $234 \equiv 2 - 3 + 4 \equiv 3 \mod 11$ and $234 \equiv 0 \mod 13$.

3. Similarly, $58473625 \equiv 210 \equiv 0 \mod 7$, $\equiv 1 \mod 11$ and $\equiv 2 \mod 13$.

4. Similarly, $100, 000, 000, 000, 000, 001 \equiv 001 - 100 \equiv -99 \equiv 6 \mod 7$, $\equiv 0 \mod 11$ and $\equiv 5 \mod 13$.

Question 14. Find divisibility tests for numbers in base 34 for $2, 3, 5, 7, 11$ and 17.

Solution:
A number in base 34 looks like this:

$$N = a_n \cdot 34^n + a_{n-1} \cdot 34^{n-1} + \cdots + a_1 \cdot 34 + a_0$$

where each coefficient a_i is a number $0 \leq a_i \leq 33$. Therefore, in this base:

1. N is divisible by 2 if a_0 is divisible by 2.

2. N is divisible by 3 if the sum of all coefficients a_i is divisible by 3 (because $34 \equiv 1 \mod 3$).

3. N is divisible by 5 if the alternating sum of the coefficients a_i is divisible by 5 (because $34 \equiv -1 \mod 5$).

4. N is divisible by 7 if the alternating sum of the coefficients a_i is divisible by 7 (because $34 \equiv -1 \mod 7$).

5. N is divisible by 11 if the sum of all coefficients a_i is divisible by 11 (because $34 \equiv 1 \mod 11$).

6. N is divisible by 17 if a_0 is 0 or 17 (because $N \equiv a_0 \mod 17$ and $0 \leq a_0 \leq 33$, so $a_0 \equiv 0 \mod 17$ iff $a_0 = 0$ or 17).

Question 15. Show that $2^{560} \equiv 1 \mod 561$.

Solution:
The best trick here is to factor $561 = 3 \cdot 11 \cdot 17$. Let's calculate first $2^{560} \mod 3, 11$ and 17.

- $2^{560} \equiv (-1)^{560} \equiv 1 \mod 3$, thus 3 divides $2^{560} - 1$.
- Modulo 11 one can verify that $2^{10} \equiv 1 \mod 11$. Thus $2^{560} \equiv (2^{10})^{56} \equiv 1 \mod 11$. Thus, 11 divides $2^{560} - 1$.
- Also, $2^8 \equiv 1 \mod 17$ and $560 = 8 \cdot 70$. Thus, $2^{560} \equiv (2^8)^7 0 \equiv 1 \mod 17$. Hence, 17 divides $2^{560} - 1$.

Therefore, $3, 11$ and 17 divide $2^{560} - 1$. Since these are distinct primes, their product also divides it. Hence 561 divides $2^{560} - 1$ and, consequently, $2^{560} \equiv 1 \mod 561$.