1. (18 points) Prove using Mathematical Induction that for all positive integers n

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}. \quad (*)$$

Case $n=1$: $\sum_{k=1}^{1} k^2 = 1^2 = 1$. $\frac{1(1+1)(2\cdot 1+1)}{6} = 1$. Equality holds.

Induction Step: Assume that equation $(*)$ holds for n.

We need to show that

$$\sum_{k=1}^{n+1} k^2 = \frac{(n+1)(n+2)(2(n+1)+1)}{6} \quad (**)$$

Left side of $(**)$ is

$$\sum_{k=1}^{n+1} k^2 = \sum_{k=1}^{n} k^2 + (n+1)^2 \overset{\text{By } (*) \text{ and the Ind. Hyp.}}{=} \frac{n(n+1)(2n+1)}{6} + (n+1)^2 =$$

$$= (n+1)\left[\frac{n(2n+1)+6(n+1)}{6}\right] = (n+1)\left[\frac{2n^2+7n+6}{6}\right]$$

Right hand side of $(**)$ is

$$(n+1)\left[\frac{(n+2)(2n+3)}{6}\right] = (n+1)\left[\frac{2n^2+7n+6}{6}\right]$$

We see that $(**)$ holds. Hence, equality $(*)$ holds by the Principle of Math. Induction. ∎

(9 pt)

2. (18 points) a) Let p be a prime and k an integer satisfying $0 < k < p$. Prove that $\binom{p}{k} \equiv 0 \pmod{p}$. Hint: Show first that p divides $\binom{p}{k} k!(p-k)!$.

$\binom{p}{k} = \frac{p!}{k!(p-k)!}$. Hence $\binom{p}{k} \cdot k! \cdot (p-k)! \overset{(*)}{=} p! = p(p-1)!$.

We proved in class that $\binom{p}{k}$ is an integer. Equality (*) shows that $p \mid \binom{p}{k} k!(p-k)!$. Hence p divides one of the three factors, since p is prime.

Now, $p \nmid k!$ and $p \nmid (p-k)!$ since both $k!$ and $(p-k)!$ are product of positive integers smaller than p.

Hence, p divides $\binom{p}{k}$. Equivalently, $\binom{p}{k} \equiv 0 \pmod{p}$.

(9 pts)

b) Let p be a prime. Prove that $(a+b)^p \equiv a^p + b^p \pmod{p}$ for all integers a, b.

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k = a^p + b^p + \sum_{k=1}^{p-1} \binom{p}{k} a^{p-k} b^k \equiv a^p + b^p \pmod{p}$$

$\binom{p}{k} \equiv 0 \pmod{p}$ by part a

Method II: The statement follows from Fermat's Little Theorem. $x^p \equiv x \pmod{p}$ for all integers x, and in particular for $x = a+b$.

3. (16 points) Use the Extended Euclidean Algorithm (E.E.A) to find the multiplicative inverse of $[71]$ in $\mathbb{Z}_{88}$. Credit will be given only for an answer using the E.E.A.

We need to solve the linear congruence

$71x \equiv 1 \pmod{88}$

we do it by solving the linear Diophantine equation

$88y + 71x = 1$

$88y_i + 71x_i = r_i$

y_i	x_i	r_i	q_i
1	0	88	—
0	1	71	—
1	-1	17	1
-4	5	3	4
21	-26	2	5
-25	31	1	1
		0	

so $88(-25) + 71 \cdot 31 = 1$

Thus $[71][31] = [1]$ in $\mathbb{Z}_{88}$ and so

$[71]^{-1} = [31]$.

4. (16 points) Find all integers x solving the simultaneous congruences

$$x \equiv 10 \pmod{43}, \quad (1)$$
$$x \equiv 11 \pmod{25}. \quad (2)$$

Justify your answer.

The hypothesis $\gcd(43,25)=1$ of the Chinese Remainder Theorem is satisfied, hence there exists a unique solution x modulo $25 \cdot 43$.

Eq (1) is equivalent to

(1)' $x + 43y = 10$, for some $y \in \mathbb{Z}$. So $x = 10 - 43y$

Equation (2) becomes

(2)' $10 - 43y \equiv 11 \pmod{25}$

$$\underbrace{-43}_{\equiv 7 \pmod{25}} y \equiv 1 \pmod{25}$$

Now $[7]^2 = [49] = [-1]$ in $\mathbb{Z}_{25}$, so $[y] = [7]^{-1} = [-7] = [18] \in \mathbb{Z}_{25}$

So $y = 18 + z \cdot 25$, for some $z \in \mathbb{Z}$.

Plugging into (1)' we get

$$x = 10 - 43(18 + 25z) = \underbrace{(10 - 43 \cdot 18)}_{\equiv \text{mod } 25 \cdot 43} - 25 \cdot 43 \cdot z$$

$10 + 43 \cdot 7 = 311$

So $x \equiv 311 \pmod{43 \cdot 25}$

The set of integer solutions is

$$\{ x \in \mathbb{Z} : x \equiv 311 \pmod{43 \cdot 25} \}$$

5. (16 points) Find the remainder when 26^{5461} is divided by $143 = 11 \cdot 13$. Justify your answer!
Hint: Use the Chinese Remainder Theorem.

We need to find $0 \le X < 143$, such that

(1) $X \equiv 26^{5461} \pmod{11 \cdot 13}$.

The hypothesis of the C.R.T $\gcd(11, 13) = 1$ is satisfied and so the C.R.T implies that the congruence (1) is equivalent to the simultaneous congruence

(2) $X \equiv 26^{5461} \pmod{11}$

(3) $X \equiv 26^{5461} \pmod{13} \iff X \equiv 0 \pmod{13}$.

Now 11 is prime and $\gcd(26, 11) = 1$, so
$26^{10} \equiv 1 \pmod{11}$, by Fermat's Little Theorem.
So $26^{5461} = 26^{5460} \cdot 26 = (26^{10})^{546} \cdot 26 \equiv 1^{546} \cdot 26 \equiv 26 \pmod{11}$
So x is the unique solution of

(2') $X \equiv 26 \pmod{11}$

(3') $X \equiv 0 \pmod{13}$

Clearly, $x_0 = 26$ is an integer solution.
Hence, the general solution is

$$X \equiv 26 \pmod{\underbrace{11 \cdot 13}_{143}}$$

The remainder of $26^{5461} \pmod{143}$ is 26.

6. (16 points) Define the relation R on the set of integers by xRy if and only if

$$(x \equiv y \pmod{11}) \text{ OR } (x \equiv y \pmod{13}).$$

Is R an equivalence relation? Prove your answer.

The relation R is NOT an equivalence relation since it is not transitive.

For example

$0 \equiv 11 \pmod{11}$, so $0 R 11$ holds

$11 \equiv -2 \pmod{13}$, so $11 R (-2)$ holds.

But $0 R (-2)$ does NOT hold, since

$0 \not\equiv -2 \pmod{11}$ and $0 \not\equiv -2 \pmod{13}$.