 1. Use induction to show that for $n \geq 1$ the partial sum

$$1^3 + 2^3 + ... + n^3 = \sum_{k=1}^{n} k^3$$

can be expressed in closed form by $\left[\frac{n(n+1)}{2}\right]^2$

Basis: $n=1$ $\quad 1^3 = 1$

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

Assume: $\displaystyle\sum_{k=1}^{n-1} k^3 = \left[\frac{(n-1)n}{2}\right]^2$

$$\sum_{k=1}^{n} k^3 = \sum_{k=1}^{n-1} k^3 + n^3 = \left[\frac{(n-1)n}{2}\right]^2 + n^3 = \frac{n^2}{2^2}\left[(n-1)^2 + 4n\right]$$

$$= \frac{n^2}{2^2}\left[n^2 - 2n + 1 + 4n\right] = \frac{n^2}{2^2}\left[n^2 + 2n + 1\right] = \frac{n^2}{2^2}(n+1)^2 = \left[\frac{n(n+1)}{2}\right]^2$$:)

2. Use Euclid's algorithm to find $(48, 22)$ and $s, t \in \mathbf{Z}$ such that $(48, 22) = 48s + 22t$.

$48 = 2 \cdot 22 + 4$ $\qquad$ solve for remainders $\qquad$ $4 = 48 - 2 \cdot 22$

$22 = 5 \cdot 4 + 2$ $\qquad\qquad\qquad\qquad\qquad$ $2 = 22 - 5 \cdot 4$

$\therefore$ $(48,22) = 2 = 22 - 5 \cdot 4 = 22 - 5(48 - 2 \cdot 22) = 11 \cdot 22 - 5 \cdot 48$

$\therefore$ $s = -5$, $t = 11$

3. Compute 3^{21} modulo 9 by repeated squaring and reduction. Show work.

Oops, a typo, I didn't mean to make it this easy

$$3^{21} = 3^{2+19} = 9 \cdot 3^{19} \equiv 0 \text{ mod } 9$$

4. Suppose R is a commutative ring (with unity) and let U be the set of all units in R.

(a) Prove that U is a multiplicative group.

(b) Prove that U cannot contain zero divisors.

(c) Describe U for the ring $\mathbf{Z}_m$ and the polynomial ring $\mathbf{R}[x]$.

a) Associativity of multiplication is inherited from R

Identity: Since $1 \cdot 1 = 1$, $1 \in U$.

Closure under multiplication: If $a, b \in U$, $\exists a', b'$ $aa' = bb' = 1$,

so $ab\,b'a' = a \cdot 1\, a' = aa' = 1$, so $ab \in U$.

Closure under inverses: If $a \in U$, $aa^{-1} = a^{-1}a = 1$, so $a^{-1} \in U$.

b) Suppose $a \in U$, $b \in R$ $ab = 0$. Then $a^{-1}ab = b = 0$:)

c) If $R = \mathbb{Z}_m$, $U = \{k \in \mathbb{Z}_m : (k, m) = 1\}$

If $R = \mathbb{R}[x]$, $U = \{p(x) \in \mathbb{R}[x] : p(x) = \text{nonzero constant}\}$

5. Partition U_{17} into cosets of $\langle 13 \rangle$.

```
> m:=17; H:=[seq(13^k mod m,k=1..4)];
                                   m := 17
                          H := [13, 16, 4, 1]
> K:=x->map(y->x*y mod m,H): K(2); K(3); K(6);
                    2H =   [9, 15, 8, 2]
                    3H =   [5, 14, 12, 3]
                    6H =   [10, 11, 7, 6]
>
```

6. Consider the set permutations on n elements $\{1, 2, \ldots n\}$ (with $n \geq 2$) that keep the element 1 fixed: $H = \{\sigma \in S_n \colon \sigma(1) = 1\}$. Prove that H is a subgroup of S_n and express the set of permutations that take 1 to 2: $K = \{\sigma \in S_n \colon \sigma(1) = 2\}$ as a coset of H.

Since $()$ preserves 1, $() \in H$

If $\sigma, \tau \in H$, then $\sigma(1) = 1$ and $\tau(1) = 1$, so $\tau^{-1}(1) = 1$,

so $\sigma\tau^{-1}(1) = \sigma(\tau^{-1}(1)) = \sigma(1) = 1$, so $\sigma\tau^{-1} \in H$ $\therefore$ $\underline{H < S_n}$

Claim: $\underline{K = (1,2)H}$. If $\sigma \in H$, then $\sigma(1) = 1$

so $(1,2)\sigma$ takes 1 to 2, so $(1,2)\sigma \in K$

Conversely, if $\tau \in K$, then $\tau(1) = 2$, so $(1,2)\tau$ takes 1 to 1, so $(1,2)\tau \in H$, so $\tau = (1,2)(1,2)\tau \in (1,2)H$

7. Prove that among the residues modulo m it is exactly those that are coprime to m that are units in the ring $\mathbb{Z}_m$.

Suppose $[n] \in \mathbb{Z}_m$ with $(n,m) = 1$. Then $\exists\, s, t \in \mathbb{Z}$

$1 = sn + mt$. Taking residues we get $[1] = [s][n]$

so $[n]$ is a unit in $\mathbb{Z}_m$.

Conversely if $[1] = [s][n]$ for some s, then

$1 \equiv sn \mod m$ so $1 = sn + mt$ for some $t \in \mathbb{Z}$

so $(n,m) = 1$

8. Find the solution set for the system of congruences

$$5x \equiv 2 \bmod 48$$

$$7x \equiv 22 \bmod 30$$

Since $5 \cdot 29 \equiv 1 \bmod 48$ and $7 \cdot 13 \equiv 1 \bmod 30$ we can multiply the 1^{st} eq. by 29 and the 2^{nd} by 13 to obtain

$$x \equiv 10 \bmod 48$$
$$x \equiv 16 \bmod 30$$

Now let's do the Euclidean algorithm on the moduli

$48 = 30 + 18$	Solve for	$18 = 48 - 30$
$30 = 18 + 12$	remainders	$12 = 30 - 18$
$18 = 12 + 6$		$6 = 18 - 12$

Since $6 \mid 18$ $(48,30) = 6 = 18 - 12 = 18 - (30 - 18)$
$= 2 \cdot 18 - 30 = 2(48 - 30) - 30 = 2 \cdot 48 - 3 \cdot 30$

So $x = 10 + 2 \cdot 48 = 106 \bmod \operatorname{lcm}(48,30) = 106 \bmod 240$

9. Exhibit (with proof) a surjective group homomorphism from the general linear group of invertible linear operators on the real plane under composition (or equivalently, 2×2 nonsingular matrices with real coefficients under matrix multiplication) $GL_2(\mathbf{R})$ to the multiplicative group of nonzero real numbers $\mathbf{R}^*$. What is this homomorphism's kernel?

$\det : GL_2(\mathbb{R}) \to \mathbb{R}^*$ is a group hom, since

$$\det(AB) = \det A \cdot \det B$$

(Note that determinant of nonsingular matrices $\neq 0$)

If $a \in \mathbb{R}^*$, then $a = \det \begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix}$ so det is onto.

$\ker \det = \{ A \in GL_2(\mathbb{R}) : \det A = 1 \}$

i.e. all area and orientation preserving linear maps.