Midterm Exam

1. (a) State the fundamental theorem of arithmetic. **(2 points)**

   (b) Let a, b, c be digits in base 10. Prove that the number $\overline{abcabc}$ is divisible by 91. **(4 points)**

   Solution. (a) The fundamental theorem of arithmetic states that any nonzero integer can be written as the product of prime powers. This form is unique up to units and the order of factors.

   (b) Observe that, for any digits a, b, c,

$$\overline{abcabc} = 1001\overline{abc} = 91 \cdot 11\overline{abc},$$

   which is clearly a multiple of 91.

2. (a) State the Chinese remainder theorem (with arbitrary many moduli). **(2 points)**

   (b) I have a few apples, not more than 200. If I try to share them between 3 kids, 2 ones are left; if I try to share them between 5 kids, 4 ones are left; if I try to share them between 7 kids, 6 ones are left. How many apples do I have? **(4 points)**

Solution. (a) Assume $m_1, \ldots, m_n$ are positive integers such that for any $1 \leqslant i < j \leqslant n$, $\gcd(m_i, m_j) = 1$. Assume further that for any $1 \leqslant i \leqslant n$, a residue class $a_i \bmod m_i$ is given. Then the Chinese remainder theorem states that there exists a unique residue class a modulo $m_1 \cdot \ldots \cdot m_n$ such that for any $1 \leqslant i \leqslant n$, $a \equiv a_i \bmod m_i$.

(b) Add one more imaginary apple. Then the new number of apples (together with the imaginary one) is divisible by $3, 5, 7$, that is, since they are pairwise coprime, by their product 105. Then the original number of apples is $105k - 1$ for some $k \in \mathbf{N}$, and if $k \geqslant 2$, the number of such apples is bigger than 200. That is, the number of apples is 104.

3. (a) State the Euler-Fermat theorem. **(2 points)**

   (b) Prove that $3^{2000} - 1$ is divisible by 10. **(4 points)**

   Solution. (a) Assume $m \in \mathbf{N}$, and a is an integer coprime to m. Then the Euler-Fermat theorem states that

$$a^{\varphi(m)} \equiv 1 \bmod m.$$

(b) Observe that

$$3^{2000} - 1 = (3^4)^{500} - 1 = 81^{500} - 1 \equiv 1^{500} - 1 = 0 \bmod 10,$$

and the proof is complete.

4. (a) State the quadratic reciprocity. **(2 points)**

   (b) Describe the prime numbers $p > 2$ which satisfy that 35 is a quadratic residue modulo p. **(4 points)**

Solution. (a) Assume that $p, q > 2$ are distinct prime numbers. Then the quadratic reciprocity states

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}},$$

where

$$\left(\frac{a}{b}\right)$$

is the Legendre symbol of a modulo b.

(b) First assume that $p \equiv 1 \bmod 4$. Then by quadratic reciprocity,

$$\left(\frac{35}{p}\right) = \left(\frac{5}{p}\right)\left(\frac{7}{p}\right) = \left(\frac{p}{5}\right)\left(\frac{p}{7}\right).$$

We need that this is 1, which holds if and only if either p is a quadratic residue modulo both 5 and 7, or it is a quadratic non-residue modulo both 5 and 7. Modulo 5, quadratic residues are $1, 4$, quadratic non-residues are $2, 3$. Modulo 7, quadratic residues aree $1, 2, 4$, quadratic non-residues are $3, 5, 6$. Together with $p \equiv 1 \bmod 4$, and applying the Chinese remainder theorem, this gives that modulo 140, p is in the set

$$\{1, 9, 13, 17, 29, 53, 73, 81, 97, 109, 121, 137\}.$$

Similarly, when $p \equiv 3 \bmod 4$,

$$\left(\frac{35}{p}\right) = \left(\frac{5}{p}\right)\left(\frac{7}{p}\right) = -\left(\frac{p}{5}\right)\left(\frac{p}{7}\right).$$

We need that this is 1, which holds if and only if p is either a quadratic residue modulo 5 (residue classes $1, 4$) and a quadratic non-residue modulo 7 (residue classes $3, 5, 6$), or it a quadratic non-residue modulo 5 (residue classes $2, 3$) and a quadratic residue modulo 7 (residue classes $1, 2, 4$). With $p \equiv -1 \bmod 4$, Chinese remainder theorem this time gives that modulo 140, p is in the set

$$\{19, 23, 31, 43, 59, 67, 107, 111, 123, 127, 131, 139\}.$$

That is, prime numbers in question are those which are congruent to an element of the displayed sets modulo 140.