Math 100A - Fall 2019 - Practice Problems for Midterm I

The midterm will cover Chapters 1.1 - 1.4 in the book. The main topics are:

- *integers, greatest common divisor, primes, fundamental theorem of arithmetic*
- *equivalence relations, congruences*
- $\mathbb{Z}_n$*, invertible elements, finding inverses via division algorithm*
- *Fermat' s theorem, Wilson's theorem*
- *permutations, cycles, transpositions, parity of permutations*

1. Consider the linear diophantine equation

$$17x + 42y = 1, \quad x, y \in \mathbb{Z}.$$

(i) Using the methods of this course, derive the general solution of this equation.
(ii) Find the inverse of 17 in $\mathbb{Z}_{42}$.
(iii) Write down all invertible elements in $\mathbb{Z}_{42}$.

2. Let $p > 5$ be a prime.

(i) Using Wilson's theorem, find $(p-2)! \mod p$.
(ii) Using (i), find $(p-3)! \mod p$.

3.

(i) Show that if x is an odd integer, then $x^2 \equiv 1 \mod 8$. Conclude that if x is any integer, then $x^2 \equiv 0, 1$ or $4 \mod 8$.
(ii) Show that if $p \equiv 3 \mod 4$ is any integer, then the equation $x^2 + y^2 = p$ has no integer solutions.
(iii) Show that if $p \equiv 7 \mod 8$ is any integer, then the equation $x^2 + y^2 + z^2 = p$ has no integer solution.

Remark: By contrast, it can be shown that if p *is any positive integer, the equation* $x^2 + y^2 + z^2 + w^2 = p$ *always has integer solutions.*

4. Show that for positive integers a, m, n we have

$$\gcd(a^m - 1, a^n - 1) = a^{\gcd(m,n)} - 1.$$

You can follow the steps below:

(i) Set $b = a^{\gcd(m,n)}$ and $k = \frac{m}{\gcd(m,n)}, \ell = \frac{n}{\gcd(m,n)}$. Show that the statement to be proved becomes

$$\gcd(b^k - 1, b^\ell - 1) = b - 1$$

whenever $\gcd(k, \ell) = 1$. Write

$$d = \gcd(b^k - 1, b^\ell - 1).$$

(ii) Prove that $b - 1 | b^k - 1$ and $b - 1 | b^\ell - 1$, and deduce $b - 1 | d$.

(iii) Conversely, show that $d | b - 1$ and conclude.

Hint: Since $\gcd(k, \ell) = 1$, we can write

$$1 = kx + \ell y$$

for integers x, y. You may have to be a bit careful that x or y may be negative.

Use that

$$b^k \equiv 1 \mod , \ b^\ell \equiv 1 \mod d$$

to conclude

$$b = b^{kx+\ell y} \equiv 1 \mod d.$$

Conclude.

5. Show that if $(a, 561) = 1$ then $a^{560} \equiv 1 \mod 561$. Since 561 is not a prime, the converse to Fermat is false.

Hint: Write $561 = 3 \cdot 11 \cdot 17$ and use Fermat for the primes $3, 11, 17$.

6. Let $a = 11^{193}$.

(i) Using Fermat's theorem, find $a \mod 13$ and $a \mod 17$.

(ii) Using (i), find $a \mod 221$.

7. Let σ be a permutation of the set $S = \{1, 2, \ldots, n\}$. For two integers $x, y \in S$, we define $x \sim y$ provided there exists an integer k such that

$$x = \sigma^k(y).$$

Show that $\sim$ is an equivalence relation.

8. Consider the permutations

$$\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 3 & 5 \end{smallmatrix}\right), \ , \tau = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{smallmatrix}\right)$$

(i) Compute $\sigma\tau$ and $\tau\sigma$.

(ii) Find the permutation χ such that

$$\sigma\chi = \tau.$$

9. Show that if σ and τ are permutations then

$$(\sigma\tau)^{-1} = \tau^{-1}\sigma^{-1}.$$

10. Consider the permutation

$$\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 4 & 10 & 5 & 7 & 8 & 2 & 6 & 9 & 1 \end{smallmatrix}\right)$$

(i) Write σ as product of cycles.

(ii) Write σ as product of transpositions.

(iii) Find the parity of σ.

11.

(i) Define the sign of the permutation

$$\operatorname{sgn}(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ even} \\ -1 & \text{if } \sigma \text{ odd} \end{cases}.$$

Show that

$$\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\tau).$$

(ii) Let σ, τ be permutations such that

$$\sigma^3 = \tau^4.$$

Using (i), show that σ is even.

(iii) Using (i), show that σ and $\tau\sigma\tau^{-1}$ have the same parity for all permutations σ and τ.

12. Please make sure to review the proofs of the theorem covered in class (e.g. Fermat's little theorem, Wilson, infinitude of primes, fundamental theorem of arithmetic etc). You may be asked to prove a statement which is similar to such theorems.

Also please review the homework problems.