Math 233, Spring 2016, Boris Botvinnik

REVIEW PROBLEMS FOR THE MIDTERM TEST II

1. Find $[a]^{-1}$ in $\mathbf{Z}_{1001}$ for $a = 33$ or prove that $[a]^{-1}$ does not exist.

2. Define the Euler function $\phi(n)$. How many non-zero divisors are there in $\mathbf{Z}_{33}$? in $\mathbf{Z}_{336}$? $\mathbf{Z}_{3367}$?

3.* Let p be a prime number. Show that $a^{p-1} \equiv 1 \bmod p$ for any positive integer $a \not\equiv 0 \bmod p$.

4. Compute the last 2 digits of 2^{166}, 3^{100}, 7^{2016}.

5.* Let p be a prime.

(i) Show that the binomial coefficient $\begin{pmatrix} p \\ k \end{pmatrix}$ is divisible by p for all $0 < k < p$.

(ii) Show that $(x+y)^p \equiv x^p + y^p \bmod p$.

6. Let a, b, c be integers such that $a^2 + b^2 + c^2 \equiv 0 \bmod 5$. Show that $a \equiv 0 \bmod 5$, or $b \equiv 0 \bmod 5$, or $c \equiv 0 \bmod 5$.

7. Find at least two different pairs of integers $0 < m, n \leq 100$ such that $7^m + 3^n$ has the last digit 8.

8. Find a general solution of the system

$$\begin{cases} x \equiv 3 \mod 5 \\ x \equiv 5 \mod 7 \\ x \equiv 7 \mod 11 \end{cases}$$

9. Solve the equations

(i) $5x \equiv 7 \bmod 99$

(ii) $9x \equiv 40 \bmod 101$

10. One uses an encryption function $E : \mathbf{Z}_{26} \to \mathbf{Z}_{26}$, where

$$E(\theta) = \alpha\theta + \kappa \mod 26.$$

It is known that $E(D) = x$ and $E(Z) = e$. Determine the function E.

11. Define the Euler function $\phi(n)$. Compute $\phi(pq)$, where p and q are prime numbers.

12.* Let a, n be positive integers and $\gcd(a, n) = 1$. Show that $a^{\phi(n)} \equiv 1 \bmod n$, where $\phi(n)$ is the Euler function.

13. Let $p = 5$, $q = 13$, $n = pq$, and you are an RSA-code manager. Which public key for a user would be a good or bad choice: e= 21, 28, 37, 43, 69, 72? Explain why.

14. Let $p = 5$, $q = 13$, $n = pq$, and you are an RSA-code manager. You have assigned a public key $e = 41$ to the user A. Give a secret key d to the same user A. Explain your choice.

15. Let p be a prime, and e be such that $\gcd(e, p-1) = 1$. Let d be such that $de \equiv 1 \mod (p-1)$. Prove that the congruence $x^e \equiv c \bmod p$ has a unique solution $x = c^d \bmod p$.

16. Compute $3^{218} \bmod 1000$.

17. Compute $7,814^{-1} \bmod 17{,}449$.

18. Compute $2^{15,485,286} \bmod 15{,}485{,}287$. Note: 15,485,287 is a prime number.

19. Solve the equation $x^2 \equiv 2 \bmod 13$.

20. Solve the equation $x^3 - x^2 + 2x - 2 \equiv 0 \bmod 11$.

21. Find all x, $0 \le x \le 34$, such that $x \equiv 1 \bmod 5$ and $x \equiv 2 \bmod 7$.

22. Find a single value x that simultaneously solves the two congruences

$$x \equiv 13 \mod 71, \quad \text{and} \quad x \equiv 41 \mod 97$$

23. Find a single value x that simultaneously solves the three congruences

$$x \equiv 4 \mod 7, \quad x \equiv 5 \mod 8, \quad \text{and} \quad x \equiv 11 \mod 15$$

24. Solve the equation $x^{1{,}583} \equiv 4,714 \bmod 7{,}919$.

Note: 7,919 is a prime number.

25. Solve the equation $x^{17{,}389} \equiv 43,927 \bmod 64{,}349$.

Note: $64,349 = 229 \cdot 281$ is a product of two prime numbers.

26. Define a Hamming code. Give an example. State and prove a necessary condition when all single errors of a Hamming code could be detected and corrected.

27. Consider a code given by the parity-check matrix

$$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

(a) What is the generator matrix of this code?

(b) How many elements does the code C have? Explain your answer.

(c) Decode the messages 1010111 and 1001000.

(d) Can all single errors in transmission be detected and corrected? Justify your answer.

(e) Explain why the minimum distance between code words is at most 2.

(f) Write down the set of code words.

(g) What is the minimum distance between code words? Justify your answer.

28. Let $n = pq$, where p and q are prime numbers. Assume you know the value $\phi(n)$, where ϕ is the Euler function. Determine p and q from n and $\phi(n)$.