ELIZABETHTOWN COLLEGE
Putnam Preparation Series
B. Doytchinov, 2007

THEME 9

1. TOPICS

Today we will talk about integer numbers, divisibility, and other questions which typically go under the rubric of *Number Theory*. More precisely, we will focus on the following topics:

1. divisibility, mod, primes, unique factorization
2. gcd, Euclid's algorithm, relatively prime numbers
3. Fermat's little theorem: $a^p \equiv a \pmod{p}$
4. Wilson's theorem: $(p-1)! \equiv 1 \pmod{p}$
5. the Chinese remainder theorem
6. Euler's ϕ function and primitive roots of n. If $(a, m) = 1$, then $a^{\phi(m)} \equiv 1 \pmod{m}$.

We will then turn our attention to *polynomials*. The ring of polynomials shares many common properties with the ring of the integers, and a lot of the theory carries over, with appropriate modifications. This is an example of the general principle that "abstract" theory is sometimes very practical.

Motivated by this, we will discuss some problems from *"Abstract" Algebra* at the end.

2. PRACTICE PROBLEMS

Number Theory

1. **(1989A1)** How many primes among the positive integers, written as usual in base 10, are such that their digits are alternating 1's and 0's, beginning and ending with 1?
2. Find integers x and y such that $754x + 221y = \gcd(754, 221)$.

3. **(1986A2)** What is the units (i.e., rightmost) digit of

$$\left\lfloor \frac{10^{20000}}{10^{100}+3} \right\rfloor ?$$

Here $\lfloor x \rfloor$ is the greatest integer $\leq x$.

4. Let a, b, c, and d be positive integers such that $ad - bc = 1$. Show that the fractions a/c, b/d, and $(a+b)/(c+d)$ are irreducible.

5. Show that $(21n+4)/(14n+3)$ is irreducible for every natural number n.

6. Prove that some positive multiple of 21 has 241 as its three final digits.

7. What are the last two digits of 3^{1234}?

8. **(1985A4)** Define a sequence $\{a_i\}$ by $a_1 = 3$ and $a_{i+1} = 3^{a_i}$ for $i \geq 1$. Which integers between 00 and 99 inclusive occur as the last two digits in the decimal expansion of infinitely many a_i?

9. **(2000A2)** Prove that there exist infinitely many integers n such that n, $n+1$, $n+2$ are each the sum of the squares of two integers. [Example: $0 = 0^2 + 0^2$, $1 = 0^2 + 1^2$, and $2 = 1^2 + 1^2$.]

10. Let a and b be relatively prime, i.e. $\gcd(a, b) = 1$. Prove the following:

    (a) $\gcd(a+b, a-b) \leq 2$

    (b) $\gcd(a+b, a-b, ab) = 1$

    (c) $\gcd(a^2 - ab + b^2, a+b) \leq 3$

11. **(2002B5)** A palindrome in base b is a positive integer whose base-b digits read the same backwards and forwards; for example, 2002 is a 4-digit palindrome in base 10. Note that 200 is not a palindrome in base 10, but it is the 3-digit palindrome 242 in base 9, and 404 in base 7. Prove that there is an integer which is a 3-digit palindrome in base b for at least 2002 different values of b.

12. **(2001A5)** Prove that there are unique positive integers a, n such that $a^{n+1} - (a+1)^n = 2001$.

13. **(2000B2)** Prove that the expression

$$\frac{\gcd(m,n)}{n}\binom{n}{m}$$

is an integer for all pairs of integers $n \geq m \geq 1$.

14. (a) Show that a perfect square must leave a remainder of 0, 1, or 4 upon division by 8. Show that it can't leave a remainder of 2 upon division by 3.

    (b) Find all pairs of integers x and y such that $x^2 + y^2 = 1999$.

    (c) With a minimum of effort, find all pairs of integers x and y such that $x^2 + y^2 = 1000$.

15. **(2000B5)** Let S_0 be a finite set of positive integers. We define finite sets $S_1, S_2, \ldots$ of positive integers as follows: the integer a is in S_{n+1} if and only if exactly one of $a-1$ or a is in S_n. Show that there exist infinitely many integers N for which $S_N = S_0 \cup \{N + a : a \in S_0\}$.

16. **(1999A6)** The sequence $(a_n)_{n\geq 1}$ is defined by $a_1 = 1, a_2 = 2, a_3 = 24$, and, for $n \geq 4$,

$$a_n = \frac{6a_{n-1}^2 a_{n-3} - 8a_{n-1}a_{n-2}^2}{a_{n-2}a_{n-3}}.$$

Show that, for all n, a_n is an integer multiple of n.

17. **(1999B6)** Let S be a finite set of integers, each greater than 1. Suppose that for each integer n there is some $s \in S$ such that $\gcd(s,n) = 1$ or $\gcd(s,n) = s$. Show that there exist $s, t \in S$ such that $\gcd(s,t)$ is prime.

18. **(1998A4)** Let $A_1 = 0$ and $A_2 = 1$. For $n > 2$, the number A_n is defined by concatenating the decimal expansions of A_{n-1} and A_{n-2} from left to right. For example $A_3 = A_2A_1 = 10$, $A_4 = A_3A_2 = 101$, $A_5 = A_4A_3 = 10110$, and so forth. Determine all n such that 11 divides A_n.

19. **(1970A3)** Find the length of the longest sequence of equal nonzero digits in which an integral square can terminate (in base 10) and find the smallest square which terminates in such a sequence.

20. **(1995A3)** The number $d_1d_2\ldots d_9$ has nine (not necessarily distinct) decimal digits. The number $e_1e_2\ldots e_9$ is such that each of the nine 9-digit numbers formed by replacing just one of the digits d_i is $d_1d_2\ldots d_9$ by the corresponding digit e_i $(1 \leq i \leq 9)$ is divisible by 7. The number $f_1f_2\ldots f_9$ is related to $e_1e_2\ldots e_9$ is the same way: that is, each of the nine numbers formed by replacing one of the e_i by the corresponding f_i is divisible by 7. Show that, for each i, $d_i - f_i$ is divisible by 7. [For example, if $d_1d_2\ldots d_9 = 199501996$, then e_6 may be 2 or 9, since 199502996 and 199509996 are multiples of 7.]

21. **(1998B6)** Prove that, for any integers a, b, c, there exists a positive integer n such that $\sqrt{n^3 + an^2 + bn + c}$ is not an integer.

22. **(1993B5)** Show there do not exist four points in the Euclidean plane such that the pairwise distances between the points are all odd integers.

23. **(1991B3)** Does there exist a real number L such that, if m and n are integers greater than L, then an $m \times n$ rectangle may be expressed as a union of 4×6 and 5×7 rectangles, any two of which intersect at most along their boundaries?

24. **(1991B5)** Let p be an odd prime and let $\mathbb{Z}_p$ denote (the field of) integers modulo p. How many elements are in the set

$$\{x^2 : x \in \mathbb{Z}_p\} \cap \{y^2 + 1 : y \in \mathbb{Z}_p\}?$$

25. **(1972A1)** Show that there are no four consecutive binomial coefficients

$$\binom{n}{r}, \qquad \binom{n}{r+1}, \qquad \binom{n}{r+2}, \qquad \binom{n}{r+3}$$

(n and r are positive integers, and $r + 3 \leq n$) which are in arithmetic progression.

26. **(1969B1)** Let n be a positive integer such that $n + 1$ is divisible by 24. Prove that the sum of the divisors of n is divisible by 24.

27. **(1982A5)** Let a, b, c, and d be positive integers and $r = 1 - a/b - c/d$. Given that $a + c \leq 1982$ and $r > 0$, prove that $r > 1/1983^3$.

28. **(1972A5)** Show that if n is an integer greater than 1, then n does not divide $2^n - 1$.

29. **(1997B5)** Prove that for $n \geq 2$,

$$\overbrace{2^{2^{\cdots^2}}}^{n \text{ times}} \equiv \overbrace{2^{2^{\cdots^2}}}^{n-1 \text{ times}} \pmod{n}.$$

30. **(1992A3)** For a given positive integer m, find all triples (n, x, y) of positive integers, with n relatively prime to m, which satisfy

$$(x^2 + y^2)^m = (xy)^n.$$

31. **(1975A1)** Supposing that an integer n is the sum of two triangular numbers $n = (a^2 + a)/2 + (b^2 + b)/2$, write $4n + 1$ as the sum of two squares, $4n + 1 = x^2 + y^2$, and show how x and y can be expressed in terms of a and b. Show that, conversely, if $4n + 1 = x^2 + y^2$, then n is the sum of two triangular numbers. (Of course, a, b, x, y are understood to be integers.)

32. **(1983A3)** Let p be an odd prime, and let

$$F(n) = 1 + 2n + 3n^2 + \cdots + (p-1)n^{p-2}.$$

Prove that if a and b are distinct integers in $\{0, 1, \ldots, p-1\}$ then $F(a)$ and $F(b)$ are not congruent modulo p, that is, $F(a) - F(b)$ is not divisible by p.

33. **(1994B6)** For any integer a, set

$$n_a = 101a - 100 \cdot 2^a.$$

Show that for $0 \leq a, b, c, d \leq 99$, $n_a + n_b \equiv n_c + n_d (\text{mod} 10100)$ implies $\{a, b\} = \{c, d\}$.

Polynomials

34. **(2000A6)** Let $f(x)$ be a polynomial with integer coefficients. Define a sequence $a_0, a_1, \ldots$ of integers such that $a_0 = 0$ and $a_{n+1} = f(a_n)$ for all $n \geq 0$. Prove that if there exists a positive integer m for which $a_m = 0$ then either $a_1 = 0$ or $a_2 = 0$.

35. **(2004B1)** Let $P(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_0$ be a polynomial with integer coefficients. Suppose that r is a rational number such that $P(r) = 0$. Show that the n numbers

$$c_n r,\ c_n r^2 + c_{n-1} r,\ c_n r^3 + c_{n-1} r^2 + c_{n-2} r, \ldots,\ c_n r^n + c_{n-1} r^{n-1} + \cdots + c_1 r$$

are integers.

36. **(2001A3)** For each integer m, consider the polynomial

$$P_m(x) = x^4 - (2m+4)x^2 + (m-2)^2.$$

For what values of m is $P_m(x)$ the product of two non-constant polynomials with integer coefficients?

37. **(1999B2)** Let $P(x)$ be a polynomial of degree n such that $P(x) = Q(x)P''(x)$, where $Q(x)$ is a quadratic polynomial and $P''(x)$ is the second derivative of $P(x)$. Show that if $P(x)$ has at least two distinct roots then it must have n distinct roots. [The roots may be either real or complex.]

38. **(1991A3)** Find all real polynomials $p(x)$ of degree $n \geq 2$ for which there exist real numbers $r_1 < r_2 < \cdots < r_n$ such that

(i) $p(r_i) = 0, \quad i = 1, 2, \ldots, n,$ and
(ii) $p'\left(\frac{r_i + r_{i+1}}{2}\right) = 0, \quad i = 1, 2, \ldots, n-1,$

where $p'(x)$ denotes the derivative of $p(x)$.

39. **(2003B4)** Let

$$f(z) = az^4 + bz^3 + cz^2 + dz + e = a(z - r_1)(z - r_2)(z - r_3)(z - r_4)$$

where a, b, c, d, e are integers, $a \neq 0$. Show that if $r_1 + r_2$ is a rational number, and if $r_1 + r_2 \neq r_3 + r_4$, then $r_1 r_2$ is a rational number.

40. **(1986B3)** Let Γ consist of all polynomials in x with integer coefficients. For f and g in Γ and m a positive integer, let $f \equiv g \pmod{m}$ mean that every coefficient of $f - g$ is an integral multiple of m. Let n and p be positive integers with p prime. Given that f, g, h, r, and s are in Γ with $rf + sg \equiv 1 \pmod{p}$ and $fg \equiv h \pmod{p}$, prove that there exist F and G in Γ with $F \equiv f \pmod{p}$, $G \equiv g \pmod{p}$, and $FG \equiv h \pmod{p^n}$.

41. **(1986B5)** Let $f(x,y,z) = x^2+y^2+z^2+xyz$. Let $p(x,y,z), q(x,y,z), r(x,y,z)$ be polynomials with real coefficients satisfying

$$f(p(x,y,z),q(x,y,z),r(x,y,z)) = f(x,y,z).$$

Prove or disprove the assertion that the sequence p,q,r consists of some permutation of $\pm x, \pm y, \pm z$, where the number of minus signs is 0 or 2.

42. **(1985B1)** Let k be the smallest positive integer with the following property:

There are distinct integers m_1, m_2, m_3, m_4, m_5 such that the polynomial

$$p(x) = (x-m_1)(x-m_2)(x-m_3)(x-m_4)(x-m_5)$$

has exactly k nonzero coefficients.

Find, with proof, a set of integers m_1, m_2, m_3, m_4, m_5 for which this minimum k is achieved.

43. **(2004A4)** Show that for any positive integer n, there is an integer N such that the product $x_1x_2\cdots x_n$ can be expressed identically in the form

$$x_1x_2\cdots x_n = \sum_{i=1}^{N} c_i(a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n)^n$$

where the c_i are rational numbers and each a_{ij} is one of the numbers $-1, 0, 1$.

44. **(1992B4)** Let $p(x)$ be a nonzero polynomial of degree less than 1992 having no nonconstant factor in common with $x^3 - x$. Let

$$\frac{d^{1992}}{dx^{1992}}\left(\frac{p(x)}{x^3-x}\right) = \frac{f(x)}{g(x)}$$

for polynomials $f(x)$ and $g(x)$. Find the smallest possible degree of $f(x)$.

45. **(1994A4)** Let A and B be 2×2 matrices with integer entries such that A, $A+B$, $A+2B$, $A+3B$, and $A+4B$ are all invertible matrices whose inverses have integer entries. Show that $A+5B$ is invertible and that its inverse has integer entries.

46. **(1987A4)** Let P be a polynomial, with real coefficients, in three variables and F be a function of two variables such that

$$P(ux, uy, uz) = u^2 F(y - x, z - x) \quad \text{for all real } x, y, z, u,$$

and such that $P(1, 0, 0) = 4$, $P(0, 1, 0) = 5$, and $P(0, 0, 1) = 6$. Also let A, B, C be complex numbers with $P(A, B, C) = 0$ and $|B - A| = 10$. Find $|C - A|$.

47. **(1985A6)** If $p(x) = a_0 + a_1 x + \cdots + a_m x^m$ is a polynomial with real coefficients a_i, then set

$$\Gamma(p(x)) = a_0^2 + a_1^2 + \cdots + a_m^2.$$

Let $f(x) = 3x^2 + 7x + 2$. Find, with proof, a polynomial $g(x)$ with real coefficients such that

(i) $g(0) = 1$, and

(ii) $\Gamma(f(x)^n) = \Gamma(g(x)^n)$

for every integer $n \geq 1$.

Abstract Algebra

48. **(1989B2)** Let S be a nonempty set with an associative operation that is left and right cancellative ($xy = xz$ implies $y = z$, and $yx = zx$ implies $y = z$). Assume that for every a in S the set $\{a^n : n = 1, 2, 3, \ldots\}$ is finite. Must S be a group?

49. **(2001A1)** Consider a set S and a binary operation $*$, i.e., for each $a, b \in S$, $a * b \in S$. Assume $(a * b) * a = b$ for all $a, b \in S$. Prove that $a * (b * a) = b$ for all $a, b \in S$.

50. **(1984B3)** Prove or disprove the following statement:
If F is a finite set with two or more elements, then there exists a binary operation $*$ on F such that for all x, y, and z in F,

(a) $x * z = y * z$ implies $x = y$ and

(b) $x * (y * z) \neq (x * y) * z$.

51. **(1987B6)** Let F be the field of p^2 elements where p is an odd prime. Suppose S is a set of $(p^2-1)/2$ distinct nonzero elements of F with the property that for each $a \neq 0$ in F, exactly one of a and $-a$ is in S. Let N be the number of elements in the intersection $S \cap \{2a : a \in S\}$. Prove that N is even.

52. **(1997A4)** Let G be a group with identity e and $\phi : G \to G$ a function such that

$$\phi(g_1)\phi(g_2)\phi(g_3) = \phi(h_1)\phi(h_2)\phi(h_3)$$

whenever $g_1g_2g_3 = e = h_1h_2h_3$. Prove that there exists an element $a \in G$ such that $\psi(x) = a\phi(x)$ is a homomorphism (that is, $\psi(xy) = \psi(x)\psi(y)$ for all $x, y \in G$).