MATH 3220 practice problems

Number theory I: Congruences, divisibility, and unique factorization

Acknowledgements

This worksheet borrows from Larson's book, the text of Gelca and Andreescu, and from material published online by Ravi Vakil, Cecil Rousseau, and Naoki Sato.

Key concepts

Unique factorization: Every natural number can be written uniquely in the form $\prod_p p^{v_p(n)}$, where p runs over primes and the exponents $v_p(n)$ are nonnegative integers, with all but finitely many $v_p(n) = 0$.

Division with remainder: For every pair of integers a, b with $b > 0$, we can write

$$a = bq + r, \quad \text{with } 0 \leq r < b.$$

Here q (the quotient) and r (the remainder) are uniquely determined.

Divisibility: If a and d are integers, we say d divides a (written $d \mid a$) if $a = dq$ for some $q \in \mathbb{Z}$. There are many useful properties of divisibility; e.g.,

(a) if $d \mid a$, then $d \mid aq$ for every q,

(b) if $d \mid a$ and $d \mid b$, then $d \mid a + b$,

(c) if $e \mid d$ and $d \mid a$, then $e \mid a$.

(d) if $d \mid ab$ and $\gcd(d, a) = 1$, then $d \mid b$.

The greatest common divisor is often important as an object in itself. One key fact about the gcd is that it can always be written as a linear combination of the starting numbers: For any a, b there are integers x, y with

$$\gcd(a, b) = ax + by.$$

Congruences: Let m be a natural number. The relation *congruence mod* m is defined as follows: Two integers a and b are *congruent mod* m, written $a \equiv b \pmod{m}$, if $m \mid b - a$. Equivalently, a and b are congruent mod m if they leave they same remainder upon division by m. For example, 1 and 7 are congruent modulo 3.

Congruence modulo m defines an equivalence relation on the set $\mathbb{Z}$ of integers. Moreover, addition and multiplication are compatible with congruences, in the following sense:

(a) If $a \equiv b \pmod{m}$ and $a' \equiv b' \pmod{m}$, then $a + a' \equiv b + b' \pmod{m}$.

(a) If $a \equiv b \pmod{m}$ and $a' \equiv b' \pmod{m}$, then $aa' \equiv bb' \pmod{m}$.

Problems

1. (a) Prove that if $m \mid a-b$ and $m \mid c-d$, then $m \mid ac-bd$. (This is asking you to prove that you can multiply congruences mod m and the result is still a true congruence modulo m; so you shouldn't assume that fact for this problem.)

   (b) Prove that polynomials with integer coefficients preserve congruences. In other words, if $f(T) \in \mathbb{Z}[T]$ is a polynomial with integer coefficients, and $m \mid a-b$, then $m \mid f(a) - f(b)$.

2. (a) Show that if $p > 3$ is a prime number, then $24 \mid p^2 - 1$.

   Hint: Every prime $p > 3$ is odd and not a multiple of 3. Now work mod 3 and mod 8 to show that both 3 and 8 divide $p^2 - 1$.

   (b) Show that there is no square whose sum of decimal digits is exactly 2013.

   Hint: Work mod 9, remembering that a number and its sum of digits are always congruent modulo 9.

   (c) If $2n+1$ and $3n+1$ are both squares, show that n is divisible by 40.

   Hint: Work mod 5 and work mod 8.

3. A Pythagorean triple consists of three positive integers a, b, and c satisfying $a^2+b^2 = c^2$. Show that 60 divides the product abc for every Pythagorean triple.

   Hint: It's enough to show that 3, 4, and 5 all divide abc.

4. Explain why a number n is divisible by 11 precisely when the alternating sum of its decimal digits is divisible by 11.

5. (*) Show that if the last four decimal digits of a square number are all equal, then they are all equal to 0. Thus, for instance, it is impossible for a square to end in 5555.

6. Prove that $2x + 3y$ is divisible by 17 if and only if $9x + 5y$ is divisible by 17.

   Hint to get you started: If $17 \mid 2x + 3y$, then 17 also divides $13(2x + 3y)\ldots$

7. Show that the fraction
$$\frac{21n+4}{14n+3}$$
   is already in lowest terms, for every $n = 1, 2, 3, \ldots$.

8. Show that if a, b, and c are any three positive integers, then
$$\gcd(a,b)\cdot\gcd(a,c)\cdot\gcd(b,c)\cdot\operatorname{lcm}[a,b,c]^2 = \operatorname{lcm}[a,b]\cdot\operatorname{lcm}[a,c]\cdot\operatorname{lcm}[b,c]\cdot\gcd(a,b,c)^2.$$

9. Suppose that $\gcd(a,b) = 1$.

   (a) Show that $\gcd(a-b, a+b) = 1$ or 2,

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

   (c) Show that $\gcd(a^2 - ab + b^2, a+b) = 1$ or 3.

10. (*) Let f be a nonconstant polynomial with positive integer coefficients. Show that for positive integers n, the number $f(n)$ divides $f(f(n)+1)$ if and only if $n=1$.

    Hint: What is $f(f(n)+1)$ modulo $f(n)$?

11. (*) Let A be the sum of the decimal digits of 4444^{4444}, and let B be the sum of the decimal digits of A. Find the sum of the decimal digits of B.

12. (*) Let m and n be positive integers. Show that if $\operatorname{lcm}[m,n]+\gcd(m,n)=m+n$, then either m divides n or vice versa.

13. (*) Let n be a positive integer for which $n+1$ is divisible by 24. Show that the sum of the positive divisors of n is also divisible by 24.

    Example: If $n=95$, the sum of the positive divisors of n is $1+5+19+95=24\cdot 5$.

14. If ab, bc, and ac are all perfect cubes, show that a, b, and c are individually also cubes.

    Hint: Show that every prime p appears to an exponent that is a multiple of 3 in each of a, b, and c.

15. Show that if a and b are positive integers where

$$a \mid b^2, \quad b^2 \mid a^3, \quad a^3 \mid b^4, \quad b^4 \mid a^5, \ldots,$$

    then $a=b$.

16. For every nonnegative integer n, put $F_n = 2^{2^n}+1$. Thus $F_0=3$, $F_1=5$, $F_2=5$, etc. These are called the *Fermat numbers*. Show that if $i \neq j$, then $\gcd(F_i, F_j)=1$.

17. (*) Three infinite arithmetic progressions are given whose terms are positive integers. Assuming that each of $1,2,3,\ldots,8$ occurs in at least one of these progressions, must it be the case that 2013 also appears in one of these progressions? Prove or give a counterexample.

18. Prove that the expression

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

    is an integer for every pair of positive integers n and m.

    Hint: First write $\gcd(n,m)$ as a linear combination of n and m.

19. (*) Prove that every positive integer can be written as a quotient of products of factorials of not-necessarily-distinct primes. For example,

$$\frac{10}{9} = \frac{2!5!}{3!\cdot 3!\cdot 3!}.$$

20. (*) Show that if n is a power of 2, then all of the middle binomial coefficients

$$\binom{n}{1}, \binom{n}{2}, \ldots, \binom{n}{n-1}$$

    are even, and that these are the only n with this property.

21. (*) Find the number of odd binomial coefficients in the list $\binom{2013}{0}, \binom{2013}{1}, \dots, \binom{2013}{2013}$.

Hint: This is simplest if you know about the arithmetic of polynomials in $(\mathbb{Z}/2\mathbb{Z})[x]$, as explained in MATH 4000. In that case, it will help to notice that

$$(x+1)^{2013} =$$
$$(x+1)^{1024}(x+1)^{512}(x+1)^{256}(x+1)^{128}(x+1)^{64}(x+1)^{16}(x+1)^{8}(x+1)^{4}(x+1),$$

and that each of the factors is easily computed mod 2.

22. (*) Show that for every positive integer n,

$$n! = \prod_{i=1}^{n} \mathrm{lcm}[1, 2, 3, \dots, \lfloor n/i \rfloor].$$

Here lcm denotes the least common multiple, and $\lfloor \cdot \rfloor$ is the usual greatest-integer function.

Hint: One way to to do this is to **carefully** compute the highest power of p dividing both the left and right-hand sides, and show that they agree for all p.

23. (a) Show that if $2^n - 1$ is prime, then n itself is prime.

Hint: Remember the algebraic identity

$$x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1}).$$

(b) Show that if $2^n + 1$ is prime, then n is a power of 2.

24. (*) Show that for every integer $n \geq 2$, if we write

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} = \frac{A}{B}$$

in lowest terms, then B is even. In particular, the left-hand side is never an integer (because in that case we would have $B = 1$).

Hint: First show that if $\frac{a}{b}$ and $\frac{c}{d}$ are fractions in lowest terms, and the highest power of 2 dividing b is larger than the highest power of 2 dividing d, then the highest power of 2 in the lowest-terms denominator of $\frac{a}{b} + \frac{c}{d}$ is the same as the highest power of 2 in b.

25. Suppose n is a positive integer, and factor n as a product of primes, say

$$n = p_1^{e_1} \cdots p_k^{e_k},$$

where the p_i are distinct primes and each e_i is a nonnegative integer.

(a) Show that the number of positive integer divisors of n is

$$(e_1 + 1)(e_2 + 1) \cdots (e_k + 1).$$

For example, since $12 = 2^2 \cdot 3$, there are $(2+1)(1+1) = 6$ positive divisors of 12. In fact, these are $1, 2, 3, 4, 6, 12$.

(b) Show that the number of solutions in positive integers x and y to the equation

$$\frac{xy}{x+y} = n$$

is precisely

$$(2e_1 + 1)(2e_2 + 1) \cdots (2e_k + 1).$$

26. (*) 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?