MATH 3220 practice problems

Number theory II: The theorems of Fermat and Euler, arithmetic functions, and miscellany

Acknowledgements

This worksheet borrows from Larson's book and the text of Gelca and Andreescu.

You may turn in any problem for credit. Especially interesting problems (to me!) are marked with an $*$.

Helpful results to keep in mind:

- **Unique factorization**: Every positive integer n can be written uniquely in the form
$$\prod_{p \text{ prime}} p^{v_p(n)},$$
where for each prime p, $p^{v_p(n)}$ is the highest power of p dividing n. Here the $v_p(n)$ are nonnegative integers and for a given n, the integer $v_p(n)$ is nonzero for only finitely many primes p. If we write
$$n = \prod_{p \text{ prime}} p^{v_p(n)} \quad \text{and} \quad m = \prod_{p \text{ prime}} p^{v_p(m)},$$
then $n \mid m$ if and only if $v_p(n) \le v_p(m)$ for each prime p. Also,
$$\gcd(n, m) = \prod_{p \text{ prime}} p^{\min\{v_p(n), v_p(m)\}} \quad \text{and} \quad \operatorname{lcm}[n, m] = \prod_{p \text{ prime}} p^{\max\{v_p(n), v_p(m)\}}.$$

- **Fermat's little theorem:** if p is prime and a is any integer, then $a^p \equiv a \pmod{p}$. If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.

- **Euler's theorem:** if a and m are relatively prime, then $a^{\phi(m)} \equiv 1 \pmod{m}$. Here $\phi(m)$ is Euler's ϕ-function, defined by
$$\phi(m) = \#\{1 \le k \le m : \gcd(k, m) = 1\}.$$

- **A formula for Euler's function:** If $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ is the decomposition of n into primes, then
$$\begin{aligned}\phi(n) &= n(1 - 1/p_1)(1 - 1/p_2) \cdots (1 - 1/p_k) \\ &= p_1^{e_1 - 1}(p_1 - 1) p_2^{e_2 - 1}(p_2 - 1) \cdots p_k^{e_k - 1}(p_k - 1).\end{aligned}$$

- **Other arithmetic functions:** We let $\tau(n)$ denote the number of positive divisors of n and $\sigma(n)$ denote the sum of the positive divisors of n. For example,
$$\tau(10) = 4 \quad \text{and} \quad \sigma(10) = 1 + 2 + 5 + 10 = 18.$$

The functions τ and σ are both **multiplicative**; we have $\tau(mn) = \tau(m)\tau(n)$ whenever $\gcd(m, n) = 1$ and also $\sigma(mn) = \sigma(m)\sigma(n)$ when $\gcd(m, n) = 1$. Moreover,

$$\tau(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}) = (e_1 + 1) \cdots (e_k + 1)$$

and

$$\sigma(p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}) = \frac{p_1^{e_1+1} - 1}{p_1 - 1} \frac{p_2^{e_2+1} - 1}{p_2 - 1} \cdots \frac{p_k^{e_k+1} - 1}{p_k - 1}.$$

Problems

1. If $p \geq 7$ is prime, show that p divides $\overbrace{111 \cdots 111}^{p-1 \text{ 1s}}$.

   Hint: Use the formula for the sum of a finite geometric series to re-express $111 \cdots 111$.

2. Find all integers n for which $n! + 5$ is a perfect cube. (One example is $n = 5$, since $5! + 5 = 125 = 5^3$.)

   Hint: A perfect cube is either not divisible by 5 or is divisible by 5^3.

3. (*) Show that every composite number (i.e., an integer > 1 that is not prime) can be written in the form
$$xy + xz + yz + 1,$$
   where x, y, and z are positive integers.

4. Determine (with proof) for which n the number $\phi(n)$ is odd. Do the same for $\sigma(n)$.

5. (*) Show that among any ten consecutive positive integers, at least one of them is relatively prime to all of the others. (Recall that two numbers are said to be relatively prime if their greatest common divisor is 1.)

6. Explain why $19 \mid 2^{2^{6k+2}} + 3$ for $k = 0, 1, 2, 3, \ldots$.

7. (*) Let p be a prime with $p > 3$. Show that p divides $2^{p-2} + 3^{p-2} + 6^{p-2} - 1$.

8. Let p be an odd prime number. Write
$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} = \frac{a}{b}$$
   in lowest terms. Show that p divides a.

9. Show that if a is any positive integer, then $a^{561} \equiv a \pmod{561}$. Note that 561 is **not** prime, in fact $561 = 3 \cdot 11 \cdot 17$.

10. Show that if $p > 17$ is prime, then $16320 \mid p^{32} - 1$.

    Hint: $16320 = 2^5 \cdot 3 \cdot 5 \cdot 17$. Use Euler's theorem to show that each of 2^5, 3, 5, and 17 divide $p^{32} - 1$.

11. Find the remainder when 2^{29} is divided by 9. If you are told that 2^{29} is missing exactly one of the digits $0, 1, 2, \ldots, 9$, use your answer to determine the missing digit (without computing 2^{29} directly).

    Hint: Use the fact that every positive integer n leaves the same remainder when divided by 9 as its sum of digits.

12. Show that if $n_1 < n_2 < \cdots < n_{31}$ are all prime numbers, and $30 \mid n_1^4 + n_2^4 + \cdots + n_{31}^4$, then $2, 3$, and 5 must all appear in the list of the n_i.

    Hint: First write out the table of 4th powers modulo 2, 3, and 5.

13. (*) Let $f(n) = 1 + 2n + 3n^2 + ... + (p-1)n^{p-2}$, where p is an odd prime. Prove that if $f(m) \equiv f(n) \pmod{p}$, then $m \equiv n \pmod{p}$.

    Hint: Using Fermat's little theorem, show that if $n \not\equiv 0$ or $1 \pmod{p}$, then $(1 - n)f(n) \equiv 1 \pmod{p}$.

14. Show that there is no solution to the equation $\phi(n) = 14$.

15. (*) Show there are infinitely many even positive integers m for which there is no solution to the equation $\phi(n) = m$. (For example, $m = 14$ is one such number.)

16. Show that the product of three consecutive positive integers is never a perfect square.

    Hint: Say the three integers are $n - 1, n$, and $n + 1$. Argue that n and $n^2 - 1$ are coprime numbers which multiply to a perfect square. Use unique factorization to show that this forces both n and $n^2 - 1$ to both be perfect squares. Why is this impossible?

17. Let n be a positive integer.

    (a) List the fractions $\frac{1}{n}, \frac{2}{n}, \ldots \frac{n}{n}$ and put each of them in lowest terms. Show that for every number d dividing n, exactly $\phi(d)$ fractions have denominator d at the end of this process.

    (b) Explain why your answer to (a) shows that $\sum_{d|n} \phi(d) = n$ for every positive integer n. Here the sum is taken over all of the divisors d of n.

    Hint: Let's experiment with $n = 30$. When put in lowest terms, the fractions become

$$\frac{1}{30}, \frac{1}{15}, \frac{1}{10}, \frac{2}{15}, \frac{1}{6}, \frac{1}{5}, \frac{7}{30}, \frac{4}{15}, \frac{3}{10}, \frac{1}{3}, \frac{11}{30}, \frac{2}{5}, \frac{13}{30}, \frac{7}{15}, \frac{1}{2}, \frac{8}{15}, \frac{17}{30}, \frac{3}{5}, \frac{19}{30}, \frac{2}{3}, \frac{7}{10}, \frac{11}{15}, \frac{23}{30}, \frac{4}{5}, \frac{5}{6}, \frac{13}{15}, \frac{9}{10}, \frac{14}{15}, \frac{29}{30}, \frac{1}{1}.$$

    There is 1 fraction with denominator 1, 1 fraction with denominator 2, 2 fractions with denominator 3, 4 fractions with denominator 5, 2 fractions with denominator 6, 4 fractions with denominator 10, 8 fractions with denominator 15, and 8 fractions with denominator 30. Also,

$$\begin{aligned} \sum_{d|n} \phi(d) &= \phi(1) + \phi(2) + \phi(3) + \phi(5)\phi(6) + \phi(10) + \phi(15) + \phi(30) \\ &= 1 + 1 + 2 + 4 + 2 + 4 + 8 + 8 = 30, \end{aligned}$$

    in agreement with the claim of part (b).

18. Let $n = 2^{31} \cdot 3^{19}$. How many positive integer divisors of n^2 are less than n but do not divide n?

Hint: Remember that the divisors of a number N always come in pairs, since if d divides N, then so does N/d. It will be useful to apply this with $N = n^2$.

19. Show that n divides $\phi(2^n - 1)$ for every positive integer n.

Hint: You might start by noticing that $2^n \equiv 1 \pmod{2^n - 1}$ and $2^{\phi(2^n-1)} \equiv 1 \pmod{2^n - 1}$.

20. (*) A natural number n is called a **perfect number** if $\sigma(n) = 2n$, where $\sigma(n)$ is the sum of the positive divisors of n. For example, 28 is perfect, since the divisors of 28 are $1, 2, 4, 7, 14, 28$, and $1 + 2 + 4 + 7 + 14 + 28 = 56 = 2 \cdot 28$.

    (a) Assume that n has the form $2^{p-1}(2^p - 1)$, where $2^p - 1$ is a prime number. Show that n is an even perfect number.

    (b) (Harder, due to Euler) Show that every even perfect number has the form given in part (a).

It is not known whether or not an odd perfect number exists, but any example has to have more than 1500 decimal digits!

21. A number n is called *squarefree* if every prime that divides n does so exactly once. For example, $30 = 2 \cdot 3 \cdot 5$ is squarefree, but $18 = 2 \cdot 3^2$ is not, since $3^2 \mid 18$. Show that 6 is the only squarefree perfect number.

22. (*) Show that every positive integer is a sum of one or more numbers of the form $2^r 3^s$, where r and s are nonnegative integers and no summand divides another. (For example, $23 = 9 + 8 + 6$.)

23. (*) Let p be a prime with $p \geq 5$. Write

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} = \frac{a}{b}$$

in lowest terms. Show that p^2 divides a. (This is a more challenging version of Exercise 8.)

24. (*) Show that there are infinitely many positive integers n with the property that $n, n+1$, and $n+2$ can both be written as the sum of two squares of integers. For example, $8 = 2^2 + 2^2$, $9 = 0^2 + 3^2$, and $10 = 1^2 + 3^2$, so $n = 8$ is such an integer.

Hint: You could try to choose $n = m^2 - 1$ where n is a sum of two squares. Then $n + 1 = m^2 + 0^2$ and $n + 2 = m^2 + 1^2$ are automatically sums of two squares. The challenge is then to show that n itself is a sum of two squares for infinitely many values of m. (I'll warn you that while this approach will work, it's not the easiest one.)

25. (*) Show that the product of four consecutive positive integers is not a perfect square.

26. Show that every positive integer has a multiple whose decimal representation has all ten digits showing up (at least once).

27. (*) Let $s(n)$ be the sum of the decimal digits of n; e.g., $s(1321) = 1+3+2+1 = 7$. Show that $s(2^n) \to \infty$ as $n \to \infty$.

    Hint: Start by showing that for every positive integer k, one can find a large positive integer m_k with the following property: 2^n always has a nonzero digit between the kth place and the m_kth place, for all but finitely many numbers n. Here the 0th place means the units digit, the 1st place means the tens digit, etc.