Primes and Dirichlet series

Berkeley Math Circle

2018-10-10

1. Euclid's proof that there are infinitely many primes repeatedly takes the smallest prime divisor of $p_1p_2...p_n+1$ where $p_1, p_2, ..$ are the primes found so far. What are the first few primes produced by this? Is $p_1p_2...p_n+1$ always prime?
2. Fix $N > 2$. Show there are infinitely many primes not of the form 1 mod N in a similar way, by looking at prime factors of $Np_1p_2..p_n - 1$. For example there are infinitely many primes whose last digit is not 1.
3. Show there are infinitely many primes that are 1 mod 2 and infinitely many that are 2 mod 3 and infinitely many that are 3 mod 4 and infinitely many that are 5 mod 6. Why does this method nor work for primes 4 mod 5?
4. Make a table of which primes can divide numbers of the form n^2+1 for n up to about 17.
5. Looking at the table of the previous exercise, can you guess a simple rule to tell which primes can divide a number of the form n^2+1? Do you think the prime 1000003 can divide a number of this form?
6. Which primes less than 30 are the sum of two squares? How does this compare with the previous exercises?
7. Show that any prime that is 3 mod 4 is not the sum of 2 squares. (It is true that all other primes are the sum of 2 squares, but this is harder to prove.)
8. Show that the nonzero integers mod p form a group (for p prime). The nontrivial part is to show that if a is not divisible by p then $ab \equiv 1 \bmod p$ for some b. Hint: Euclid's algorithm.
9. The number 5 has order exactly 4 mod 13 ($5^4 \equiv 1 \bmod 13$). Find the 3 cosets $\{n, 5n, 5^2n, 5^3n\}$ mod 13 explicitly, and check that the nonzero integers mod 13 are the disjoint union of these 3 cosets. Deduce that 4 divides $13-1$.
10. Lagrange's theorem: Show that if x has order exactly k mod p for p prime then k divides $p-1$. (Generalize the previous exercise.)

11. Use Lagrange's theorem to show that if p (prime) divides $n^2 + 1$ then either $p = 2$ or 4 divides $p - 1$.

12. Show that there are infinitely many primes of the form 1 mod 4 by imitating Euclid's proof that there are infinitely many primes. (Hint: $(p_1 p_2 ...)^2 + 1$)

13. Do the same for primes dividing $n^2 + n + 1$. In other words make a table of primes dividing such numbers, and guess a rule for which primes have this property. Use this to show there are infinitely many primes that are 1 mod 3.

14. And for $n^4 + n^3 + n^2 + n + 1$. Can you use this to prove a result about primes mod 5?

15. Suppose q is prime. Show that if p divides $(n^q - 1)/(n - 1)$ then p is either q or is 1 mod q. Show that there are infinitely many primes that are 1 mod p.

16. The Riemann zeta function
$$\zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots$$
. Show Euler's result that
$$\zeta(s) = \frac{1}{1 - 2^{-s}} \frac{1}{1 - 3^{-s}} \frac{1}{1 - 5^{-s}} \frac{1}{1 - 7^{-s}} \cdots$$
where the product is over all primes. This is really the fundamental theorem of arithmetic.

17. Show that $\zeta(1)$ is infinite (it is the harmonic series). Deduce that the number of primes is infinite by looking at Euler's product for $\zeta(s)$

18. Put
$$L(s) = \frac{1}{1^s} - \frac{1}{3^s} + \frac{1}{5^s} - \cdots$$
Show that
$$L(s) = \frac{1}{(1 + 3^{-s})(1 - 5^{-s})(1 + 7^{-s})(1 + 11^{-s}) \cdots}$$
where the sign is + for primes that are 3 mod 4 and $-$ for primes that are 1 mod 4.

19. Show that $L(1)$ is finite and nonzero (in fact it is $\pi/4$).

20. Show that $\zeta(s)/L(s)$ is infinite at $s = 1$. Use this to show that there are infinitely many primes of the form 3 mod 4. Similarly show that $\zeta(s)L(s)$ is infinite at $s = 1$ and deduce there are infinitely many primes of the form 1 mod 4.

    So we see that there are infinitely many primes that are 1 or 3 mod 4 because the series $1 - 1/3 + 1/5 - 1/7 \cdots$ is nonzero!

21. A Dirichlet character of order N is a function χ from integers to complex numbers such that

   - $\chi(n+N) = \chi(n)$
   - $\chi(1) = 1$
   - $\chi(n) = 0$ unless n is coprime to N
   - $\chi(mn) = \chi(m)\chi)n)$

   Find all Dirichlet characters mod 1,2,3,4,5,6,7,8,9.

22. Show that if χ is a Dirichlet character then

$$\sum_n \frac{\chi(n)}{n^s} = \prod_p \frac{1}{1 - \chi(p)p^{-s}}$$

   The sum on the left is called a Dirichlet series $L(\chi, s)$.

23. Check that for each Dirichlet character you found above that $L(\chi, 1) \neq 1$, and is finite except for the characters that are 0 or 1 everywhere.

24. Use the 4 Dirichlet L-series mod 8 to show that there are infinitely many primes that are 7 mod 8. (Look at $L(\chi_1, s)L(\chi_7, s)/L(\chi_3, s)L(\chi_5, s)$ where χ_3, χ_5, χ_7 are 1 on 1 and (3, 5, 7), and -1 elsewhere.)