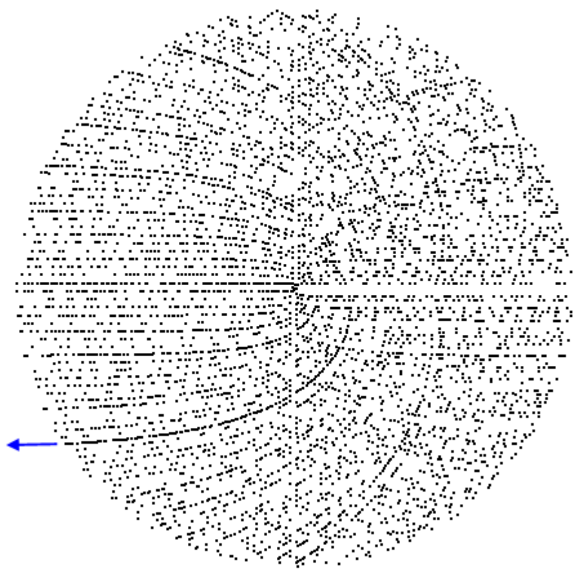
Primo Primes

Colorado Math Circle

October 24, 2009



1. Find all the prime numbers less than 100 using the *Sieve of Eratosthenes* method. How many are there? (Find $\pi(100)$.)

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

2. Let $\gcd(m, n)$ represent the greatest common divisor of m and n. Let $\text{lcm}(m, n)$ represent the least common multiple of m and n.

   (a) Prime factor 84 and 126.

   (b) Find $\gcd(84, 126)$.

   (c) Find $\text{lcm}(84, 126)$.

   (d) Confirm that $\gcd(84, 126) \cdot \text{lcm}(84, 126) = 84 \cdot 126$.

   (e) Explain why the product of the gcd and the lcm equals the product of the original numbers: $\gcd(m, n) \cdot \text{lcm}(m, n) = m \cdot n$.

3. Euclidean Algorithm.

   (a) Find $\gcd(2025, 600)$ first by using prime factorization, then by using the algorithm.

   (b) Find $\gcd(21, 13)$. Do you notice a pattern?

   (c) Find $\gcd(F_n, F_{n-1})$ where F_n and F_{n-1} are consecutive Fibonacci numbers. How many steps does the algorithm take?

4. A pair of primes that differ by 2 are called *twin primes*. Find the first 5 pairs of twin primes.

5. A *semiprime* (or *biprime*) is a composite number that is the product of two primes (that may be equal). The first three semiprimes are $4, 6, 9$. Find the next three.

6. The *Goldbach Conjecture* states that every even integer greater than 2 can be written as the sum of two primes. Express 28, 40, and 96 as the sum of two primes. Are there multiple solutions?

7. Show that the *Fermat numbers* $2^n + 1$ are prime for $n = 1, 2, 4, 8$.

8. Show that the *Mersenne numbers* $2^n - 1$ are composite for $n = 4, 9, 10$.
   Show that the Mersenne numbers $2^p - 1$ are prime for $p = 2, 3, 5, 7$.

9. Fermat claimed that every prime of the form $4n + 1$ can be uniquely written as the sum of two squares. Express 17 and 73 as the sum of two squares.

10. Euler showed that $n^2 - n + 41$ produces a prime number for all integers n from 0 to 40. Show that this polynomial does indeed generate a prime for $n = 5, 6, 7$. Show that this polynomial generates a composite number for $n = 41$.

11. *Fermat's Little Theorem* states that p divides evenly into $a^p - a$. Show that this is true for 9^3 and 4^5.

$$a^p \equiv a \pmod{p}$$

12. The Euler totient function $\varphi(n)$ equals the number of integers less than or equal to n (including 1) that are relatively prime to n. For example, $\varphi(6) = 2$ and $\varphi(9) = 6$.

    Find $\varphi(n)$ for $n = 12, 13, 14, 15$.

    Find $\varphi(p)$ for prime p.

13. Wilson's Theorem states that p is prime if and only if p divides evenly into $(p-1)! + 1$. For example, for $p = 3$ divides evenly into $2! + 1$. Show that this is true for $p = 5, 7$.

$$(p-1)! \equiv -1 \pmod{p}$$

14. More Euclidean Algorithm problems.

    (a) When does the algorithm end in two steps?

    (b) Find $\gcd(2n + 13, n + 7)$.

    (c) Prove that the fraction $\frac{12n+1}{30n+2}$ cannot be reduced for any natural number n.

    (d) Find $\gcd(2^{120} - 1, 2^{100} - 1)$.

15. More Euler's totient function problems.

    (a) Find $\varphi(p^2)$ for prime p.

    (b) Find a formula for $\varphi(n)$ when n is a semiprime that equals pq for distinct primes p and q.

    (c) Let n be a positive integer. Compute $\varphi(d)$ of every divisor d of n and add the results. What do you get?

    (d) Add all the positive integers smaller than n and relatively prime to n. What do you get?

    (e) Prove Wilson's Theorem.

    (Hint: If p is prime, the numbers $2, 3, \ldots, p-2$ can be paired up so that each pair has a product of 1 (mod p). For example, if $p = 7$, the numbers $2, 3, 4, 5$ can be paired up as follows: $2 \cdot 4 \equiv 1 \pmod{7}$ and $3 \cdot 5 \equiv 1 \pmod{7}$.)

16. *In the early morning, astronomers spiritualized nonmathematicians* is a mnemonic for the first seven primes. Create your own mnemonic for the first few primes.