WORKSHEET 6

Prime Numbers

DEFINITION. A positive integer $p \geq 2$ is said to be *prime* if it is not divisible by any positive integer other than 1 and itself. A positive integer $n \geq 2$ that is not prime is said to be *composite*.

PROBLEM 6.1. Write down the first 20 primes.

PROBLEM 6.2. Show that if m is a positive integer greater than 1, then two consecutive positive integers n and $n+1$ cannot both be divisible by m.

PROBLEM 6.3. Show that if $m_1, m_2, \ldots, m_r$ are finitely many positive integers, then there is a positive integer divisible by all of $m_1, m_2, \ldots, m_r$.

PROBLEM 6.4. Show that if $p_1, p_2, \ldots, p_r$ is any finite list of primes, then there is a positive integer not divisible by any of $p_1, \ldots, p_r$.

PROBLEM 6.5. Show that there are infinitely many primes.

PROBLEM 6.6. Show that there are infinitely many primes that leave a remainder of 3 when divided by 4.

→ P in the form 4n+1 makes a composite number 4n+1 when squared Use this to show that there is at least one prime of the form 4n+3 in any chosen set/list.

PROBLEM 6.7. Show that there are infinitely many primes that leave a remainder of 2 when divided by 3.

PROBLEM 6.8. Show that for any positive integer n, there are n consecutive composite numbers.

PROBLEM 6.9. Let $f(n) = n^2 - n + 41$. Compute $f(0), f(1), f(2), \ldots, f(10)$. Observe that all these numbers are primes. Does there exist a positive integer n such that $f(n)$ is composite?

PROBLEM 6.10. Does there exist a nonconstant polynomial $f(n)$ with integer coefficients such that $|f(n)|$ is never composite for any integer n?

PROBLEM 6.11. Find all the prime factors of the numbers $2^2 - 1$, $2^4 - 1$, $2^6 - 1$, $2^8 - 1$, and $2^{10} - 1$.

PROBLEM 6.12. Find all the prime factors of the numbers $2^3 - 1$, $2^6 - 1$, $2^9 - 1$, $2^{12} - 1$, and $2^{15} - 1$.

PROBLEM 6.13. Show that if n is a positive integer and $2^n - 1$ is prime, then n is prime.

Numbers of the form $2^n - 1$ are called *Mersenne numbers*, and primes of this form are called *Mersenne primes*.

PROBLEM 6.14. Does there exist a prime number p such that $2^p - 1$ is composite? → Yes, 11 for ex.

PROBLEM 6.15. Show that if n is a positive integer and $2^n + 1$ is prime, then n is a power of 2.

Numbers of the form $2^{2^n} + 1$ are called *Fermat numbers*. Fermat thought that $2^{2^n} + 1$ was prime for all nonnegative integers n, but $n = 5$ is a counterexample: we have $2^{2^5} + 1 = 641 \times 6700417$.

PROBLEM 6.16. Suppose you wish to check if 1003 is prime. What do you need to check? If you're going to check this by testing if it's divisible by each number for a while, do you have to go all the way up to 1002, or can you guarantee that it's prime by stopping at some earlier point? Generalize your findings.

* I meant to say N = 4 (list multiplied) -1.00ps!

Problem Set 6: Prime Numbers

Alexander Friesen 10/28-11/2, 2025

6.1: 2, 3, 5, 7, 11, 13, 17, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73.

6.2: The only number that divides n and n+1 evenly is 1, and because m>1 m must divide only n, not n+1.

6.3: Multiply all numbers from m_1 to m_r together!

6.4: Multiply all primes together and add 1!

6.5: Say that there is a list of finite prime numbers, as in 6.4. From 6.4's answer we can create another prime, p_{r+1}. But if we call this prime p_r and move the whole list down 1 index of prime, then we get another new list of primes! Because this process can be repeated forever, there are infinitely many primes.

6.6: Assume the list of 4n+3 primes is finite. It is possible to create another 4n+3 number, N, by multiplying the whole list together* but it could or could not be prime. (cont.)

6.6 (cont.). But we know that N must be odd - 2 isn't in the form $4n+3$ and it is the only possible even prime factor. This means that either (or both) $4n+1$ and/or $4n+3 (= 4n-1)$ divides N. Because two factors of the form $4n+1$ create another "$4n+1$" when multiplied together, there must be at least one prime factor of N in the form $4n+3$ - because otherwise $N \neq 4n+3$ while $N = 4n+1$, an invalid case. However, this one minimum prime factor cannot be in the original set, because none divide N - only $N+1$. This means that our list of $4n+3$ primes was incomplete, indicating that it must be infinite by repeating this.

*or any multiple of 41, in fact.

6.7: Again, begin with a proof by contradiction.

- Make N 3(the whole list multiplied together)+2.
- Note that the only other option to be a prime factor of N is 3n+1 other than 3n+2.
- Going through the same contradiction as with the 4n+3 problem, there must be another missed prime factor of 3n+2 in our list - but our list never had that new prime factor, therefore it must be infinite.

6.8: Suppose we have a list of numbers:
$(n+1)!+2, (n+1)!+3, \ldots (n+1!)+15, \ldots (n+1)!+(n+1)$.
Every number in this sequence must be composite because it must be divisible by the number adding to it. Of course, n can be any number, proving that (at least from this list) there is infitude in lengths of consecutive composite numbers.

6.9: In order from F(0) to F(10): 41, 41, 43, 47, 53, 61, 71, 83, 97, 113, and 131. Yes, composite occurs at n=41.*

*okay, there are a few special cases that pale to the big picture.

6.10: NO - making n equal the constant (without the f(n) being a constant) always gives a composite answer.*

6.11: In order again: (3), (3,5), (7,3,3), (3,5,17), (3,11,31).

6.12: In order again: (7), (7,3,3), (7,73), (7,3,3,5,13), (7,31,151).

6.13: Let's say that n is composite while 2^n-1 is prime. In this case, $n=ab \neq 1$. $2^n-1=2^{ab}-1=(2^a)^b-1$. But a core algebraic theorem states that 2^x-1 is divisible by 2^y-1 as long as $x>y$ and $\frac{x}{y}$ is a whole number. This shows that $2^n-1=(2^a)^b-1$ is divisible by 2^a-1, and because $2^a-1 \neq 1$, 2^n-1 is composite. This contradicts 2^n-1's primeness, meaning that n must be prime and not composite.

6.14: 11 is the smallest example: $2^{11}-1=2047=23 \cdot 89$.

6.15: Any n can be written as (when an integer) $2^x \cdot y$, and as long as y is odd this is true. This means that $2^n+1=2^{2^x \cdot y}+1$. However, the rule from 6.13 still works when y is >1, and $2^{2^x \cdot y}+1$ is composite unless $y=1$, meaning that only $2^{2^x}+1$ (Fermat #s) can be prime.

*1003 ÷ 17 = 59.

6.16: Because each factor pair for any n never goes above $\sqrt{n}$ (for the smaller factor), you only need to check factors below $\sqrt{n}$ to see if n is prime or not. You can also use base prime numbers to eliminate checking composite numbers below $\sqrt{n}$, so all you need to check for division of n is every prime below $\sqrt{n}$. For 1003 this looks like:

$\sqrt{1003} = 31.670175244 2\ldots \approx 31.$

So we check if 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, and 31 divide 1003. 17 divides 1003 evenly*, therefore it is not prime. (This approach is basically a cheat code to prime factorization as long as you have a calculator.)