

PT. Primarity Tests

Given an natural number n , we want to determine if n is a prime number.

(PT.1) If a number m of the form $m = 2^n - 1$, where $n \in \mathbf{N}$, is a **Mersenne number**. If a Mersenne number m is also a prime, then m is called a **Mersenne prime**.

Open Problem: Are there infinitely many Mersenne primes?

Lucas-Lehmer Test is one to test if a Mersenne number is a Mersenne prime.

(i) **Input:** $M_n = 2^n - 1$, with $n \geq 3$.

(ii) **Computing:** Set $s_1 = 4$, and for $j = 2, \dots, n - 1$, compute

$$s_j \equiv s_{j-1}^2 - 1 \pmod{M_n},$$

(iii) **Conclusion:** If $s_{n-1} \equiv 0 \pmod{M_n}$, then M_n is a Mersenne prime; otherwise M_n is not a prime.

(PT. 2) **Example:** Determine if $m = M_{13} = 2^{13} - 1 = 8191$ is a Mersenne prime.

j	$s_j \pmod{m}$	j	$s_j \pmod{m}$
1	4	7	1857
2	14	8	36
3	194	9	1294
4	4870	10	3470
5	3953	11	128
6	5970	12	0

We conclude that m is a Mersenne prime.

(PT. 3) **Exercise:** Use Lucas-Lehmer Test to verify that $M_7 = 2^7 - 1 = 127$ is a prime.

(PT. 4) **Exercise:** Use Lucas-Lehmer Test to test which of the following number is a prime and which is not: $M_9 = 511$, $M_{10} = 1023$, $M_{11} = 2047$, M_j , $3 \leq j \leq 20$.

(PT. 5) The following formula is often useful to determine if a number $b^n - 1$ is a prime or not: When $d|n$, writing $N = n/d$, we have

$$b^n - 1 = (b^d)^N - 1 = (b^d - 1)((b^d)^{N-1} + (b^d)^{N-2} + \dots + (b^d)^2 + b^d + 1).$$

(i) If n is a composite number, say $n = ds$, then by the formula in (PT. 4),

$$2^n - 1 = (2^d - 1)((2^d)^{s-1} + \cdots + 2^d + 1).$$

For example, $511 = 2^9 - 1 = (2^3 - 1)(2^6 + 2^3 + 1)$ is not a prime.

(PT. 6) **Primerity Test of $b^n - 1$:**

(PT.6A) Let $b > 1$. Then for any two positive integers m, n ,

$$\gcd(b^m - 1, b^n - 1) = b^{\gcd(m, n)} - 1.$$

Proof: We argue by induction on $\max\{m, n\}$. If $m = n$ or if $\max\{m, n\} = 1$, the assertion holds trivially.

Assume that $m - n \geq 1$ and that the statement holds for smaller values of $\max\{m, n\}$. Without loss of generality, we assume that $m > n$. Note that when $m > n$,

$$(b^m - 1) - b^{m-n}(b^n - 1) = b^{m-n} - 1.$$

Thus if an integer d divides two of the three integers $b^m - 1$, $b^n - 1$ and $b^{m-n} - 1$, then d divides the third. It follows that

$$\gcd(b^m - 1, b^n - 1) = \gcd(b^n - 1, b^{m-n} - 1).$$

Since $m > n$, $\max\{m - n, n\} < \max\{m, n\}$. By induction,

$$\gcd(b^m - 1, b^n - 1) = \gcd(b^n - 1, b^{m-n} - 1) = b^{\gcd(m, m-n)} - 1.$$

What is left is to show that $\gcd(m, m - n) = \gcd(m, n)$.

(PT.6B) Fix a positive integer b . Let n be a positive integer. If a prime p divides $b^n - 1$, then either $p|b^d - 1$ for some proper factor $d > 1$ of n , or $p \equiv 1 \pmod{n}$.

Proof: By Fermat, $b^{p-1} \equiv 1 \pmod{p}$, and so $p|(b^p - 1)$. Since $p|(b^n - 1)$, by (PT. 6A), $p|b^{\gcd(n, p-1)} - 1$. Let $d = \gcd(n, p - 1)$.

If $d < n$, then d is a proper factor of n . If $d = n$, then $n|p-1$ and so $p \equiv 1 \pmod{n}$.

(PT.6C) When p is odd and n is odd, we have $2|p - 1$. Since $\gcd(2, n) = 1$, if $n|p - 1$, we also have $(2n)|(p - 1)$, and so $p \equiv 1 \pmod{2n}$.

(PT.6D) The following formula is often useful to determine if a number $2^n - 1$ is a Mersenne prime or not: When $d|n$, writing $N = n/d$, we have

$$b^n - 1 = (b^d)^N - 1 = (b^d - 1)((b^d)^{N-1} + (b^d)^{N-2} + \cdots + (b^d)^2 + b^d + 1).$$

(ii) Is $m = 127 = 2^7 - 1$ a prime? Let p be a smallest prime dividing m . Then $p \leq \sqrt{127} < \sqrt{144} = 12$. Since 7 is a prime, by (PT.6C) with $b = 2$ and $n = 7$, if p is a prime factor of 127, then it must be $p \equiv 1 \pmod{7}$ or $p \equiv 1 \pmod{14}$. No such prime exists and so 127 is a prime.

(iii) Is $m = 2047 = 2^{11} - 1$ a prime? Let p be a smallest prime dividing m . Then $p \leq \sqrt{2^{12}} < 2^6 = 64$ (a bit too big, isn't it?). By (PT.6B) with $n = 11$ and $b = 2$, either $p|11$ or both $p \equiv 1 \pmod{11}$ and $p \equiv 1 \pmod{22}$. One such possible p is $p = 23$. Division yields $2047/23 = 89$, and so $2047 = (23)(89)$.

(iv) Is $m = 131071 = 2^{17} - 1$ a prime? Let p be a smallest prime dividing m . Then $p \leq \sqrt{m} < \sqrt{131769} = 363$ (a bit too big, isn't it?). By (PT.6B) with $n = 17$ and $b = 2$, either $p|17$ or both $p \equiv 1 \pmod{17}$ and $p \equiv 1 \pmod{34}$. Considering such possible numbers of the form $34k + 1$ that are less than 363: 35, 69, 103, 137, 171, 205, 239, 273, 307, 341.

Among these numbers, taking away those that are composite numbers:

$$5|35, 3|69, 3|171, 5|205, 3|273, 11|341,$$

we have 103, 137, 239, 307 left.

Check each of the survivors to see if any of them is a factor of m : $131071 \equiv 55 \pmod{103}$, $131071 \equiv 99 \pmod{137}$, $131071 \equiv 99 \pmod{239}$, and $131071 \equiv 289 \pmod{307}$. Hence none is a factor of m , which implies that m is a Mersenne prime.

(v) If $n = 2k > 0$ is an even number, then

$$b^n - 1 = (b^k)^2 - 1 = (b^k - 1)(b^k + 1).$$

As an example, $3^4 - 1 = (3^2 - 1)(3^2 + 1) = (3 - 1)(3 + 1)(2)(5) = (2)^4(5)$.

(vi) If b is an odd number, then $2|(b^n - 1)$. Thus $3^7 - 1 = 2186 = (2)(1093)$. Apply (PT.6B) to this case with $b = 3$ and $n = 7$, if p is a smallest prime dividing $3^7 - 1$, then $p \equiv 1 \pmod{7}$. As $2|3^7 - 1$, and as $\gcd(2, p) = 1$, we also have $p \equiv 1 \pmod{14}$. Also, $p \leq \sqrt{1093} < \sqrt{1156} = 34$. Need to test 15, 29. As 15 is not a prime, we only consider 29. Since $1093 \equiv 20 \pmod{29}$, 1093 is a prime and so we have the complete factorization of $3^7 - 1$ into primes: $3^7 - 1 = (2)(1093)$.

(PT. 7) **Pocklington's Theorem** Let $n = ab + 1$ with $a, b \in \mathbf{N}$ and $b > 1$. If for any prime factor q with $q|b$, $\exists m \in \mathbf{Z}$ such that both $m^{n-1} \equiv 1 \pmod{n}$ and $\gcd(m^{(n-1)/q} - 1, n) = 1$, then each of the following holds.

(i) For any prime p with $p|b$, $p \equiv 1 \pmod{b}$.

(ii) If $b > \sqrt{n} - 1$, then n is a prime.

Proof: (Omitted).

(PT. 8) **Example:** Use Pocklington's Theorem to test $n = 104759$ for primality, knowing that the prime $q = 52379$ is a factor of $n - 1$.

(Step 1) **Checking applicability:** Compute to get $n - 1 = 2q$ and so $n = 2q + 1$. (Thus n has the form $n = ab + 1$. If n does not have such a form, the theorem cannot be used for this purpose). Note that $b = q > 1$ and q is the only prime with $q|b$.

(Step 2) **Choosing m :** Choose $m = 2$ (This is done by trial and error. We usually start the trial with smaller numbers). Compute $m^{n-1} \equiv 2^{104758} \equiv 1 \pmod{n}$, and $\gcd(m^{(n-1)/q} - 1, n) = \gcd(2^4 - 1, n) = 1$. (So $m = 2$ works).

(Step 3) **Verifying condition:** Compute to see that $b = q > \sqrt{n}$, and conclude that n is a prime.

(PT. 9) **Powers and roots modulo m** Let $m, n \in \mathbf{N}$ and $c \in \mathbf{Z}$ with $\gcd(c, n) = 1$. If for some $x \in \mathbf{Z}$, $x^m \equiv c \pmod{n}$, then c is the m th power of $x \pmod{n}$, and x is the m th root \pmod{n} . A square (2nd power) mod n is also called a **quadratic residue** \pmod{n} .

(PT. 10) **Example:** Since $1^2 \equiv 6^2 \equiv 1, 2^2 \equiv 5^2 \equiv 4, 3^2 \equiv 4^2 \equiv 2 \pmod{7}$, 1, 2 and 4 are quadratic residue mod 7; and 3, 5 are quadratic non-residues mod 7.

(PT. 11) **Proth's Theorem** Let $k, t \in \mathbf{N}$ with t odd and $2^k > t$. Then $n = 2^k t + 1$ is a prime if and only if for some quadratic non-residues $c \pmod{n}$, $c^{(n-1)/2} \equiv -1 \pmod{n}$.

Proof: (Omitted).

(PT. 12) **Example:** Use Proth's Theorem to test $n = 13313$ for primality. (Assume that we know $c = 3$ is a quadratic non-residues mod n).

(Step 1) **Checking applicability:** $n - 1 = 2^{10} \cdot 13$, and so $n = 2^{10} \cdot 13 + 1$ has the form $n = 2^k t + 1$, where $k = 10$ and $t = 13$.

(Step 2) **Verifying condition:** $c = 3$, and compute to see $3^{(n-1)/2} = 3^{6656} \equiv -1 \pmod{n}$. Therefore, by Proth's Theorem, n is a prime.

(PT. 13) **Converse of Fermat's Little Theorem** If $n \in \mathbf{N}$ with $n > 2$, then n is prime if and only if for some $m \in \mathbf{N}$,

$$m^{n-1} \equiv 1 \pmod{n}, \text{ but } \forall \text{ prime } p|(n-1), m^{n-1}/p \not\equiv 1 \pmod{n}.$$

Proof: (Omitted).

(PT. 14) **Example:** Use (PT. 11) to test $n = 16487$ for primality.

(Step 1) **Choosing m :** Compute $n - 1 = 2 \cdot 8243 = 2q$ where $q = 8243$ is a prime. We choose $m = 2$ (by trial and error, starting with smaller numbers. Note that 2 and q are the only proper factors of $n - 1$).

(Step 2) **Verifying conditions:** Compute $m^{n-1} \equiv 2^{16486} \equiv 1 \pmod{n}$; $2^2 \not\equiv 1$ and $2^{8243} \not\equiv 1 \pmod{n}$. Therefore, n is a prime.

(PT. 15) **When an integer is a composite?** Let n be an integer. Suppose that there exist integers x, y such that $x^2 \equiv y^2 \pmod{n}$ but $x \not\equiv \pm y \pmod{n}$. Then each of the following holds.

(i) n is a composite.

(ii) Let $d = \gcd(x - y, n)$. Then $1 < d < n$.

Proof: Use the property that if n is a prime and if $n|ab$, then $n|a$ or $n|b$ (with $a = x - y$ and $b = x + y$) to see that n must be a composite. $d = n \implies n|x - y \implies x \equiv y \pmod{n}$. Thus assume $d = 1$. (Use the property that if $\gcd(a, b) = 1$ and if $a|bc$, then $a|c$). From $n|(x^2 - y^2) = (x - y)(x + y)$ and $d = 1$, we have $n|(x + y) \implies x \equiv -y \pmod{n}$.

(PT. 16) Example: For $n = 3837523$, we have been told the following

$$\begin{aligned} 9398^2 &\equiv 5^5 \cdot 19 \pmod{n} \\ 19095^2 &\equiv 2^2 \cdot 5 \cdot 11 \cdot 13 \cdot 19 \pmod{n} \\ 1964^2 &\equiv 3^2 \cdot 13^3 \pmod{n} \\ 17078^2 &\equiv 2^6 \cdot 3^2 \cdot 11 \pmod{n} \end{aligned}$$

Multiply these relations side by side to get

$$\begin{aligned} (9398 \cdot 19095 \cdot 1964 \cdot 17078)^2 &\equiv (2^4 \cdot 3^2 \cdot 5^3 \cdot 11 \cdot 13^2 \cdot 19)^2 \pmod{n} \\ 2230387^2 &\equiv 2586705^2 \pmod{n}. \end{aligned}$$

Let $x = 2230387$ and $y = 2586705$. We verify that $x \not\equiv \pm y \pmod{n}$. Then we can factor n by computing

$$(x - y, n) = (2586705 - 2230387, 3837523) = 1093, \text{ and } \frac{3837523}{1093} = 3511.$$

Hence $n = 3837523 = (1093)(3511)$.

(PT. 17) Example: As $7^2 \equiv 2^2 \pmod{15}$ and $7 \not\equiv \pm 2 \pmod{15}$, we conclude that 15 is a composite, and $5 = \gcd(7 - 2, 15)$ is a nontrivial factor of 15.

(PT. 18) **When an integer is a composite?** We apply Fermat's Little Theorem (2.12), which states that if $p > 2$ is a prime, then $2^{p-1} \equiv 1 \pmod{p}$. Suppose that 12 is a prime, then we should have $2^{11} \equiv 1 \pmod{12}$. If this is not true, then 12 is a composite. Perform these computation:

$$\begin{aligned} 2^4 &= 16 \equiv 4 \equiv 2^2 \pmod{12} \\ 2^8 &= (2^4)^2 \equiv (2^2)^2 \equiv 2^2 \pmod{12} \\ 2^{12} &= (2^8)(2^4) \equiv (2^2)(2^2) \equiv 2^2 \not\equiv_{12} 1 \pmod{12} \end{aligned}$$

Thus 12 must be a composite. (This example is extended to the next test).

(PT. 19) **Miller-Selfridge-Robin (MSR) Primality Test.**

Input: An odd integer $n > 1$ such that for some integer $k \geq 0$ and odd integer m , $n - 1 = 2^k m$.

Initialization: Choose a random integer a with $1 < a < n - 1$. Compute $b_0 \equiv a^m \pmod{n}$. If $b_0 \equiv \pm 1 \pmod{n}$, then STOP and output the message that n is probably a prime. Otherwise continue.

Iteration: FOR $i = 1, 2, \dots, k$, DO

Set $b_i \equiv b_{i-1}^2 \pmod{n}$.

IF $b_i \equiv 1 \pmod{n}$, THEN STOP and output the message that n is a composite, and that $\gcd(b_{i-1} - 1, n)$ is a nontrivial factor of n .

IF $b_i \equiv -1 \pmod{n}$, THEN STOP and output the message that n is probably a prime.

OTHERWISE continue.

Reason: If $b_i \equiv 1 \pmod{n}$ but $b_{i-1} \not\equiv \pm 1 \pmod{n}$, then

$$(b_{i-1} - 1)(b_{i-1} + 1) \equiv (b_{i-1}^2 - 1) \equiv b_i - 1 \equiv 0 \pmod{n}$$

and so view $x = b_{i-1}$ and $y = 1$ to see that if n were a prime, then at Step $i - 1$, either $b_{i-1} \equiv 1$ or $b_{i-1} \equiv -1 \pmod{n}$, and so the Algorithm must have stopped. Since the algorithm did not stopped, we must have $x \not\equiv_n \pm y$, and so by (PT. 13), $d = \gcd(x - y, n) = \gcd(b_{i-1} - 1, n)$ must be a proper factor of n .

(PT. 20) **Example:** Test if $n = 561$ is a composite. Then $n - 1 = 560 = 16 \cdot 35$, and so $2^k = 2^4$, $k = 4$ and $m = 35$. Pick $a = 2$. Then

$$\begin{aligned} b_0 &\equiv 2^{35} \equiv 263 \pmod{561} \\ b_1 &\equiv b_0^2 \equiv 166 \pmod{561} \\ b_2 &\equiv b_1^2 \equiv 67 \pmod{561} \\ b_3 &\equiv b_2^2 \equiv 1 \pmod{561} \end{aligned}$$

Thus 561 is a composite and $(b_2 - 1, n) = (66, 561) = 33$ is a factor of 561.

(PT. 21) If n is a composite and for some a with $1 < a < n - 1$, $a^{n-1} \equiv 1 \pmod{n}$, then n is called a **pseudo prime** for the base a (or a **pseudo prime** to the base a). If, in addition, that n passes the Miller-Robin test, then n is called a **strong pseudo prime** for the base a . (In other words, pseudo primes are numbers that pretend to be primes).

(PT. 22) **Example:** $n = 561$ is a pseudo prime for the base 2, but it is not a strong pseudo prime for the base 2.

(PT. 22) **Example:** $n = 91$ is a pseudo prime for the base 3, as $3^{90} \equiv 1 \pmod{91}$. But 91 is not a strong pseudo prime for the base 2, because $2^{90} \equiv 64 \pmod{91}$. (In fact, from $2^{90} \equiv 64 \pmod{91}$ we know that 91 is not a prime.)

(PT. 23) **Exercise:** Find all bases b for which 15 is a pseudo prime.