- **Strong pseudoprimes.** Suppose n is an odd composite number and write $n - 1 = 2^s m$ where m is an odd integer. Then n is a *strong pseudoprime to the base b* if either (i) $b^m \equiv 1 \pmod{n}$ or (ii) $b^{2^j m} \equiv -1 \pmod{n}$ for some $j \in [0, s-1]$.

  Two strong pseudoprimes base 2: 1093^2 and 3511^2

Maple's "isprime" Routine (Version 5, Release 3)

Comment: Each of isprime(1093^2) and isprime(3511^2) in Maple V, Release 3, ends up in an infinite loop.

The help output for isprime:

FUNCTION: isprime - primality test

CALLING SEQUENCE:
  isprime(n)

PARAMETERS:
  n - integer

SYNOPSIS:

- The function isprime is a probabilistic primality testing routine.

- It returns false if n is shown to be composite within within one strong pseudo-primality test and one Lucas test and returns true otherwise. If isprime returns true, n is "very probably" prime - see Knuth "The art of computer programming", Vol 2, 2nd edition, Section 4.5.4, Algorithm P for a reference and H. Reisel, "Prime numbers and computer methods for factorization". No counter example is known and it has been conjectured

FUNCTION: isprime - primality test

CALLING SEQUENCE:

isprime(n)

PARAMETERS:

n - integer

SYNOPSIS:

- The function isprime is a probabilistic primality testing routine.

- It returns false if n is shown to be composite within within one strong pseudo-primality test and one Lucas test and returns true otherwise. If isprime returns true, n is "very probably" prime - see Knuth "The art of computer programming", Vol 2, 2nd edition, Section 4.5.4, Algorithm P for a reference and H. Reisel, "Prime numbers and computer methods for factorization". No counter example is known and it has been conjectured that such a counter example must be hundreds of digits long.

SEE ALSO: nextprime, prevprime, ithprime

The Lucas-Lehmer Primality Test

Fix integers P and Q. Let $D = P^2 - 4Q$. Define recursively u_n and v_n by

$$u_0 = 0, \quad u_1 = 1, \quad u_{n+1} = Pu_n - Qu_{n-1} \text{ for } n \geq 1,$$

$$v_0 = 2, \quad v_1 = P, \quad \text{and} \quad v_{n+1} = Pv_n - Qv_{n-1} \text{ for } n \geq 1.$$

If p is an odd prime and $p \nmid PQ$ and $D^{(p-1)/2} \equiv -1 \pmod{p}$, then $p | u_{p+1}$.

Compute u_{n+1} quickly and check if $n | u_{n+1}$. If not, then n is composite. If so, then it is likely n is prime.

How do we compute u_{n+1} quickly?

Why does $p | u_{p+1}$ if p is an odd prime?

Why should we think n is likely a prime if $n | u_{n+1}$?

Fix integers P and Q. Let $D = P^2 - 4Q$. Define recursively u_n and v_n by

$$u_0 = 0, \quad u_1 = 1, \quad u_{n+1} = Pu_n - Qu_{n-1} \text{ for } n \geq 1,$$

$$v_0 = 2, \quad v_1 = P, \quad \text{and} \quad v_{n+1} = Pv_n - Qv_{n-1} \text{ for } n \geq 1.$$

If p is an odd prime and $p \nmid PQ$ and $D^{(p-1)/2} \equiv -1 \pmod{p}$, then $p | u_{p+1}$.

How do we compute u_{n+1} quickly?

Compute u_n modulo p by using

$$\begin{pmatrix} u_{n+1} & v_{n+1} \\ u_n & v_n \end{pmatrix} = M^n \begin{pmatrix} 1 & P \\ 0 & 2 \end{pmatrix} \quad \text{where} \quad M = \begin{pmatrix} P & -Q \\ 1 & 0 \end{pmatrix}.$$

Fix integers P and Q. Let $D = P^2 - 4Q$. Define recursively u_n and v_n by

$$u_0 = 0, \quad u_1 = 1, \quad u_{n+1} = Pu_n - Qu_{n-1} \text{ for } n \geq 1,$$

$$v_0 = 2, \quad v_1 = P, \quad \text{and} \quad v_{n+1} = Pv_n - Qv_{n-1} \text{ for } n \geq 1.$$

If p is an odd prime and $p \nmid PQ$ and $D^{(p-1)/2} \equiv -1 \pmod{p}$, then $p | u_{p+1}$.

Why does $p | u_{p+1}$ if p is an odd prime?

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{and} \quad v_n = \alpha^n + \beta^n \quad \text{for } n \geq 0,$$

where $\alpha = (P + \sqrt{D})/2$ and $\beta = (P - \sqrt{D})/2$

Why does $p | u_{p+1}$ if p is an odd prime? $D^{(p-1)/2} \equiv -1 \pmod{p}$

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{and} \quad v_n = \alpha^n + \beta^n \quad \text{for } n \geq 0,$$

where $\alpha = (P + \sqrt{D})/2$ and $\beta = (P - \sqrt{D})/2$

$$2^n \sqrt{D}\, u_n = 2^n \alpha^n - 2^n \beta^n = \left(P + \sqrt{D}\,\right)^n - \left(P - \sqrt{D}\,\right)^n$$

$$2^n \alpha^n = \left(P + \sqrt{D}\,\right)^n = \sum_{j=0}^{n} \binom{n}{j} P^{n-j} \sqrt{D}^j$$

$$2^n \beta^n = \left(P - \sqrt{D}\,\right)^n = \sum_{j=0}^{n} \binom{n}{j} P^{n-j} (-\sqrt{D}\,)^j$$

$$2^n \alpha^n - 2^n \beta^n = 2\left(\binom{n}{1} P^{n-1} \sqrt{D}^1 + \binom{n}{3} P^{n-3} \sqrt{D}^3 + \cdots \right)$$

$$= 2\sqrt{D}\left(\binom{n}{1} P^{n-1} + \binom{n}{3} P^{n-3} \sqrt{D}^2 + \cdots \right)$$

Why does $p|u_{p+1}$ if p is an odd prime?

$D^{(p-1)/2} \equiv -1 \pmod p$

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{and} \quad v_n = \alpha^n + \beta^n \quad \text{for } n \geq 0,$$

where $\alpha = (P + \sqrt{D})/2$ and $\beta = (P - \sqrt{D})/2$

$$2^n \sqrt{D}\, u_n = 2^n\alpha^n - 2^n\beta^n = \left(P + \sqrt{D}\,\right)^n - \left(P - \sqrt{D}\,\right)^n$$

$$2^n \sqrt{D}\, u_n = 2\sqrt{D}\left(\binom{n}{1}P^{n-1} + \binom{n}{3}P^{n-3}D + \binom{n}{5}P^{n-5}D^2 + \cdots\right)$$

$$2^{n-1} u_n = \binom{n}{1}P^{n-1} + \binom{n}{3}P^{n-3}D + \binom{n}{5}P^{n-5}D^2 + \cdots$$

$$2^n\alpha^n - 2^n\beta^n = 2\left(\binom{n}{1}P^{n-1}\sqrt{D}^1 + \binom{n}{3}P^{n-3}\sqrt{D}^3 + \cdots\right)$$

$$= 2\sqrt{D}\left(\binom{n}{1}P^{n-1} + \binom{n}{3}P^{n-3}\sqrt{D}^2 + \cdots\right)$$

Why does $p|u_{p+1}$ if p is an odd prime? $D^{(p-1)/2} \equiv -1 \pmod{p}$

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{and} \quad v_n = \alpha^n + \beta^n \quad \text{for } n \geq 0,$$

where $\alpha = (P + \sqrt{D})/2$ and $\beta = (P - \sqrt{D})/2$

$$2^n \sqrt{D}\, u_n = 2^n \alpha^n - 2^n \beta^n = \left(P + \sqrt{D}\,\right)^n - \left(P - \sqrt{D}\,\right)^n$$

$$2^n \sqrt{D}\, u_n = 2\sqrt{D}\left(\binom{n}{1} P^{n-1} + \binom{n}{3} P^{n-3} D + \binom{n}{5} P^{n-5} D^2 + \cdots\right)$$

$$2^{n-1} u_n = \binom{n}{1} P^{n-1} + \binom{n}{3} P^{n-3} D + \binom{n}{5} P^{n-5} D^2 + \cdots$$

$$2^p u_{p+1} = \binom{p+1}{1} P^p + \binom{p+1}{3} P^{p-2} D + \binom{p+1}{5} P^{p-4} D^2 + \cdots$$

$$2^p u_{p+1} = \binom{p+1}{1} P^p + \binom{p+1}{3} P^{p-2} D + \cdots + \binom{p+1}{p} P D^{(p-1)/2}$$

Why does $p|u_{p+1}$ if p is an odd prime? $D^{(p-1)/2} \equiv -1 \pmod{p}$

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{and} \quad v_n = \alpha^n + \beta^n \quad \text{for } n \geq 0,$$

$$\text{where } \alpha = (P + \sqrt{D})/2 \text{ and } \beta = (P - \sqrt{D})/2$$

$$2^{n-1} u_n = \binom{n}{1} P^{n-1} + \binom{n}{3} P^{n-3} D + \binom{n}{5} P^{n-5} D^2 + \cdots$$

$$2^p u_{p+1} = \binom{p+1}{1} P^p + \binom{p+1}{3} P^{p-2} D + \binom{p+1}{5} P^{p-4} D^2 + \cdots$$

$$2^p u_{p+1} = \binom{p+1}{1} P^p + \binom{p+1}{3} P^{p-2} D + \cdots + \binom{p+1}{p} P D^{(p-1)/2}$$

$$2^p u_{p+1} \equiv P^p + P D^{(p-1)/2} \pmod{p}$$

Why does $p|u_{p+1}$ if p is an odd prime?

$$D^{(p-1)/2} \equiv -1 \pmod{p}$$

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{and} \quad v_n = \alpha^n + \beta^n \quad \text{for } n \geq 0,$$

where $\alpha = (P + \sqrt{D})/2$ and $\beta = (P - \sqrt{D})/2$

$$2^{n-1} u_n = \binom{n}{1} P^{n-1} + \binom{n}{3} P^{n-3} D + \binom{n}{5} P^{n-5} D^2 + \cdots$$

$$2^p u_{p+1} = \binom{p+1}{1} P^p + \binom{p+1}{3} P^{p-2} D + \binom{p+1}{5} P^{p-4} D^2 + \cdots$$

$$2^p u_{p+1} = \binom{p+1}{1} P^p + \binom{p+1}{3} P^{p-2} D + \cdots + \binom{p+1}{p} P D^{(p-1)/2}$$

$$2^p u_{p+1} \equiv P^p + P D^{(p-1)/2} \equiv P - P \equiv 0 \pmod{p}$$

Fix integers P and Q. Let $D = P^2 - 4Q$. Define recursively u_n and v_n by

$$u_0 = 0, \quad u_1 = 1, \quad u_{n+1} = Pu_n - Qu_{n-1} \text{ for } n \geq 1,$$

$$v_0 = 2, \quad v_1 = P, \quad \text{and} \quad v_{n+1} = Pv_n - Qv_{n-1} \text{ for } n \geq 1.$$

If p is an odd prime and $p \nmid PQ$ and $D^{(p-1)/2} \equiv -1 \pmod{p}$, then $p | u_{p+1}$.

Why does $p | u_{p+1}$ if p is an odd prime?

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{and} \quad v_n = \alpha^n + \beta^n \quad \text{for } n \geq 0,$$

where $\alpha = (P + \sqrt{D})/2$ and $\beta = (P - \sqrt{D})/2$

$$2^{n-1} u_n = \binom{n}{1} P^{n-1} + \binom{n}{3} P^{n-3} D + \binom{n}{5} P^{n-5} D^2 + \cdots$$

$$\implies \quad p | u_{p+1}$$

Fix integers P and Q. Let $D = P^2 - 4Q$. Define recursively u_n and v_n by

$$u_0 = 0, \quad u_1 = 1, \quad u_{n+1} = Pu_n - Qu_{n-1} \text{ for } n \geq 1,$$

$$v_0 = 2, \quad v_1 = P, \quad \text{and} \quad v_{n+1} = Pv_n - Qv_{n-1} \text{ for } n \geq 1.$$

If p is an odd prime and $p \nmid PQ$ and $D^{(p-1)/2} \equiv -1 \pmod{p}$, then $p | u_{p+1}$.

Maple's Version

- Take $Q = 1$.
- Find first P where the Jacobi symbol $\left(\frac{P^2 - 4}{n}\right) = -1$.
- Should check if n is a square (recall 1093 and 3511).
- Make use of the identities, where $n \geq 1$.

$$v_{2n} = v_n^2 - 2, \quad v_{2n+1} = v_{n+1}v_n - P, \quad Du_n = 2v_{n+1} - Pv_n$$

$$v_{2n} = v_n^2 - 2, \quad v_{2n+1} = v_{n+1}v_n - P, \quad Du_n = 2v_{n+1} - Pv_n$$

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{and} \quad v_n = \alpha^n + \beta^n \quad \text{for } n \geq 0,$$

where $\alpha = (P + \sqrt{P^2 - 4})/2$ and $\beta = (P - \sqrt{P^2 - 4})/2$

$$\alpha\beta = 1 \implies v_{2n} = v_n^2 - 2$$

$$\alpha + \beta = P \implies v_{2n+1} = v_{n+1}v_n - P$$

$$\alpha - \beta = \sqrt{D}, \quad 2\alpha - P = \sqrt{D}, \quad 2\beta - P = -\sqrt{D}$$

$$\implies \sqrt{D}\,(\alpha^n - \beta^n) = 2(\alpha^{n+1} + \beta^{n+1}) - P(\alpha^n + \beta^n)$$

$$\implies Du_n = 2v_{n+1} - Pv_n$$

Fix integers P and Q. Let $D = P^2 - 4Q$. Define recursively u_n and v_n by

$$u_0 = 0, \quad u_1 = 1, \quad u_{n+1} = Pu_n - Qu_{n-1} \text{ for } n \geq 1,$$

$$v_0 = 2, \quad v_1 = P, \quad \text{and} \quad v_{n+1} = Pv_n - Qv_{n-1} \text{ for } n \geq 1.$$

If p is an odd prime and $p \nmid PQ$ and $D^{(p-1)/2} \equiv -1 \pmod{p}$, then $p | u_{p+1}$.

Maple's Version

- Take $Q = 1$.
- Find first P where the Jacobi symbol $\left(\dfrac{P^2 - 4}{n}\right) = -1$.
- Should check if n is a square (recall 1093 and 3511).
- Make use of the identities, where $n \geq 1$.

$$v_{2n} = v_n^2 - 2, \quad v_{2n+1} = v_{n+1}v_n - P, \quad Du_n = 2v_{n+1} - Pv_n$$

Maple's Version

- Take $Q = 1$.
- Find first P where the Jacobi symbol $\left(\frac{P^2 - 4}{n}\right) = -1$.
- Make use of the identities, where $n \geq 1$.

$$v_{2n} = v_n^2 - 2, \quad v_{2n+1} = v_{n+1}v_n - P, \quad Du_n = 2v_{n+1} - Pv_n$$

- Also, $u_p \equiv -1 \pmod{p}$ and $(v_{p+1}, v_p) \equiv (2, P) \pmod{p}$.

$$\sqrt{D}\, 2^p u_p = (P + \sqrt{D})^p - (P - \sqrt{D})^p \implies u_p \equiv -1 \pmod{p}$$

$$2^p v_p = (P + \sqrt{D})^p + (P - \sqrt{D})^p \implies v_p \equiv P \pmod{p}$$

$$Du_p = 2v_{p+1} - Pv_p \implies v_{p+1} \equiv 2 \pmod{p}$$

Maple's Version

- Take $Q = 1$.
- Find first P where the Jacobi symbol $\left(\frac{P^2-4}{n}\right) = -1$.
- Make use of the identities, where $n \geq 1$.

$$v_{2n} = v_n^2 - 2, \quad v_{2n+1} = v_{n+1}v_n - P, \quad Du_n = 2v_{n+1} - Pv_n$$

- Also, $u_p \equiv -1 \pmod{p}$ and $(v_{p+1}, v_p) \equiv (2, P) \pmod{p}$.
- Maple checks if $(v_{n+1}, v_n) \equiv (2, P) \pmod{n}$.
- If so, then $v_{n+2} \equiv P \pmod{n}$ which implies $n | u_{n+1}$.

Two lines left in isprime routine:

```
for p from 3 while (numtheory[jacobi])(p^2-4,n) <> -1 do od;
evalb(`isprime/TraceModQF`(p,n+1,n) = [2, p])
```

Maple's Version

- Take $Q = 1$.
- Find first P where the Jacobi symbol $\left(\frac{P^2-4}{n}\right) = -1$.

Fix integers P and Q. Let $D = P^2 - 4Q$. Define recursively u_n and v_n by

$$u_0 = 0, \quad u_1 = 1, \quad u_{n+1} = Pu_n - Qu_{n-1} \text{ for } n \geq 1,$$

$$v_0 = 2, \quad v_1 = P, \quad \text{and} \quad v_{n+1} = Pv_n - Qv_{n-1} \text{ for } n \geq 1.$$

If p is an odd prime and $p \nmid PQ$ and $D^{(p-1)/2} \equiv -1 \pmod{p}$, then $p | u_{p+1}$.

Two lines left in isprime routine:

```
for p from 3 while (numtheory[jacobi])(p^2-4,n) <> -1 do od;
evalb(`isprime/TraceModQF`(p,n+1,n) = [2, p])
```

Maple's Version

- Take $Q = 1$.
- Find first P where the Jacobi symbol $\left(\frac{P^2-4}{n}\right) = -1$.
- Make use of the identities, where $n \geq 1$.

$$v_{2n} = v_n^2 - 2, \quad v_{2n+1} = v_{n+1}v_n - P, \quad Du_n = 2v_{n+1} - Pv_n$$

- Also, $u_p \equiv -1 \pmod{p}$ and $(v_{p+1}, v_p) \equiv (2, P) \pmod{p}$.
- Maple checks if $(v_{n+1}, v_n) \equiv (2, P) \pmod{n}$.
- If so, then $v_{n+2} \equiv P \pmod{n}$ which implies $n | u_{n+1}$.

evalb(‘isprime/TraceModQF‘(p,n+1,n) = [2, p])

```
TraceModQF := proc ( p, k, n )
local i, kk, trc, v;
option
   `Copyright (c) 1993 Gaston Gonnet, Wissenschaftl. Rechnen, ETH Zurich. All rights
reserved.`;
kk := k;
for i while kk > 1 do kk := iquo(kk+1,2,v[i]) od;
trc := [ p, 2 ];
for i from i-1 by -1 to 1 do
   if v[i]=1 then
      trc := modp( [trc[1]^2 - 2, trc[1]*trc[2] - p], n );
   else trc := modp( [trc[1]*trc[2] - p, trc[2]^2 - 2], n );
   fi
od;
trc
end:
```

- **Make use of the identities, where $n \geq 1$.**

$$v_{2n} = v_n^2 - 2, \quad v_{2n+1} = v_{n+1}v_n - P, \quad Du_n = 2v_{n+1} - Pv_n$$

- **Maple checks if $(v_{n+1}, v_n) \equiv (2, P) \pmod{n}$.**

$$n = (v'_{i-1}v'_{i-2}\ldots v'_2v'_1)_2$$

trc := [p, 2]; $\longleftarrow (v_1, v_0)$

```
for i from i-1 by -1 to 1 do
    if v[i]=1 then
        trc := modp( [trc[1]ˆ 2 - 2, trc[1]*trc[2] - p], n );
    else trc := modp( [trc[1]*trc[2] - p, trc[2]ˆ 2 - 2], n );
    fi
od;
trc
```

$$v_{2n} = v_n^2 - 2, \quad v_{2n+1} = v_{n+1}v_n - P, \quad Du_n = 2v_{n+1} - Pv_n$$

Claim: Beginning with (v_1, v_0) and the left-most bit of n, (v_{m+1}, v_m) is replaced by (v_{2m+2}, v_{2m+1}) whenever the bit 1 is encountered and by (v_{2m+1}, v_{2m}) otherwise.

- Maple checks if $(v_{n+1}, v_n) \equiv (2, P) \pmod{n}$.

$n = (v'_{i-1}v'_{i-2}\ldots v'_2v'_1)_2$

```
trc := [ p, 2 ];   ⟵ (v1, v0)
for i from i-1 by -1 to 1 do
   if v[i]=1 then
      trc := modp( [trc[1]ˆ2 - 2, trc[1]*trc[2] - p], n );
   else trc := modp( [trc[1]*trc[2] - p, trc[2]ˆ2 - 2], n );
   fi
od;
trc
```

evalb(‘isprime/TraceModQF‘(p,n+1,n) = [2, p])

Mersenne Primes

The Lucas-Lehmer Test. ***Let p be an odd prime, and define recursively***

$$L_0 = 4 \quad \text{and} \quad L_{n+1} = L_n^2 - 2 \pmod{(2^p - 1)} \quad \text{for} \quad n \geq 0.$$

Then $2^p - 1$ is a prime if and only if $L_{p-2} = 0$.