Homework (due Friday, 09/21/18):

Page 7: Problems 3 & 4

Probable Primes and the Like

- **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 $j \in [0, s-1]$.**

- **There are no n which are strong pseudoprimes to every base b with $1 \leq b \leq n$ and $\gcd(b, n) = 1$.**

- **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

```
> n := 3511^2
                    n := 12327121
> ifactor(n - 1);
              (2)^4 (3)^3 (5) (13) (439)
```

- **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

```
> n := 1093^2
```

$$n := 1194649$$

```
> ifactor(n - 1);
```

$$(2)^3\,(3)\,(7)\,(13)\,(547)$$

- **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

> $n := 1093^2$

$$n := 1194649$$

> $ifactor(n-1);$

$$(2)^3\,(3)\,(7)\,(13)\,(547)$$

> $m := \dfrac{n-1}{8}$

$$m := 149331$$

> $2^m \ \mathbf{mod}\ n;$

$$823592$$

> $2^{2\cdot m} \ \mathbf{mod}\ n;$

$$1194648$$

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

Comment: Each of isprime(1093ˆ2) and isprime(3511ˆ2) in Maple V, Release 3, ends up in an infinite loop.

> $isprime(785678197);$

$$true$$

> $isprime(1093^2);$

$$false$$

> $isprime(3511^2);$

$$false$$

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

Comment: Each of isprime(1093ˆ2) and isprime(3511ˆ2) 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 $p | u_{p+1}$.

Idea: Given a large positive integer n, if n is prime, there is a 50-50 chance that a D will satisfy $D^{(p-1)/2} \equiv -1 \pmod{n}$. Play with P and Q until you find such a D with $n \nmid PQ$. 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.

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 $\beta = (P - \sqrt{D})/2$

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