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

Page 7: Problems 3 & 4

Probable Primes and the Like

- The use of Fermat's Little Theorem
- The example $341 = 11 \times 31$
- The example $561 = 3 \times 11 \times 17$
- Some noteworthy estimates:

$$P_2(x) \le x^{1-\frac{\log\log\log x}{2\log\log x}} \quad \text{and} \quad C(x) \le x^{1-\frac{\log\log\log x}{\log\log x}}$$

$$C(x) \ge x^{2/7} \quad \forall x \ge x_0$$

$$\pi(x) \ge \frac{x}{\log x} = x^{1-\frac{\log\log x}{\log x}} \quad \forall x \ge 17$$

$$P_2(2.5 \times 10^{10}) = 21853 \quad \text{and} \quad \pi(2.5 \times 10^{10}) = 1091987405$$

Probable Primes and the Like

Definition. A Carmichael number is a composite $n \in \mathbb{Z}^+$ for which $a^{n-1} \equiv 1 \pmod{n}$ for all integers a relatively prime to n.

Theorem: *A composite $n \in \mathbb{Z}^+$ is a Carmichael number if and only if both (i) n is squarefree, and (ii) for every prime p dividing n, $(p-1)|(n-1)$.*

Theorem. *A composite $n \in \mathbb{Z}^+$ is a Carmichael number if and only if $a^n \equiv a \pmod{n}$ for all integers a.*

Theorem. *A composite $n \in \mathbb{Z}^+$ is a Carmichael number if and only if n is odd and $a^{n-1} \equiv 1 \pmod{n}$ for all integers a relatively prime to n.*

Theorem. *A composite $n \in \mathbb{Z}^+$ is a Carmichael number if and only if n is odd and $a^n \equiv a \pmod{n}$ for all integers a.*

Probable Primes and the Like

- **There are infinitely many absolute pseudoprimes**

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

- **Strong pseudoprimes base b are pseudoprimes base b.**

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 $j \in [0, s-1]$.**
- **Strong pseudoprimes base b are pseudoprimes base b.**

```
> 2^340 mod 341
                                1
> ifactor(340)
                        (2)^2 (5) (17)
> 2^85 mod 341
                               32
> 2^170 mod 341
                                1
```

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 $j \in [0, s-1]$.
- Strong pseudoprimes base b are pseudoprimes base b.
- Primes p satisfy (i) or (ii) for any b relatively prime to p.
- There are no n which are strong pseudoprimes to every base b with $1 \leq b \leq n$ and $\gcd(b, n) = 1$.

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 $1 \le b \le n$ and $\gcd(b,n) = 1$.

Assume otherwise. Note that n must be squarefree. Next, consider a prime divisor q of n, and note $n/q > 1$. Let $c \in [1, q-1]$ be such that c is not a square modulo q. Let b satisfy $b \equiv 1 \pmod{n/q}$ and $b \equiv c \pmod{q}$. Then (i) cannot hold modulo q and (ii) cannot hold modulo n/q.

- $5^{280} \equiv 67 \pmod{561}$

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 $\gcd(b, n) = 1$.

- $5^{280} \equiv 67 \pmod{561}$

- The number $3215031751 = 151 \times 751 \times 28351$ is simultaneously a strong pseudoprime to each of the bases 2, 3, 5, and 7. It's the only such number $\leq 2.5 \times 10^{10}$.

$$b^{p-1} \equiv 1 \pmod{p} \implies b^{(p-1)/2} \equiv \pm 1 \pmod{p}$$

$$x^2 \equiv 1 \pmod{p} \implies x \equiv \pm 1 \pmod{p}$$

What about for composite n (instead of p)?

If $b^{n-1} \equiv 1 \pmod{n}$ with n odd and composite, then what is the probability that $b^{(n-1)/2} \equiv \pm 1 \pmod{n}$?

$$b^{n-1} \equiv 1 \pmod{n} \implies b^{(n-1)/2} \equiv \,??\, \pmod{n}$$

$$x^2 \equiv 1 \pmod{n} \implies x \equiv \,??\, \pmod{n}$$

What if $n = p^k$ with p an odd prime?

$$x^2 \equiv 1 \pmod{p^k} \implies x \equiv \pm 1 \pmod{p^k}$$