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

- **Teminology: pseudoprime, probable prime, industrial grade prime, absolute pseudoprime, Carmichael number**
- **The equivalence of different definitions for absolute pseudoprimes**

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, $(p-1)|(n-1)$.*

Probable Primes and the Like

- **Teminology: pseudoprime, probable prime, industrial grade prime, absolute pseudoprime, Carmichael number**
- **The equivalence of different definitions for absolute pseudoprimes**

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, $(p-1)|(n-1)$.***

Probable Primes and the Like

- **Teminology: pseudoprime, probable prime, industrial grade prime, absolute pseudoprime, Carmichael number**
- **The equivalence of different definitions for absolute pseudoprimes**

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.***