MATH 56 WORKSHEET : factorization basics

Barnett
5/9/13

A) Find a factor of $3^{300}+1$:

B) Simplifying exponentiation mod k : explain why the 2nd equality holds:

$$507^{123} \pmod{14} = (14\times 36+3)^{123} \pmod{14} = 3^{123} \pmod{14}$$

Hence state a preliminary step to make expmodk more efficient.

C) Use Euclid's algorithm to compute $\gcd(2261, 1275)$ by hand:

D) Factor 8051 [Hint: how close is it to 8100?]

Barnett
5/9/13

MATH 56 WORKSHEET : factorization basics

SOLUTIONS

A) Find <u>a</u> factor of $\underbrace{3^{300}}_{x^3} + 1$: for $x = 3^{100}$

$x+1$ is a factor, ie $3^{100}+1$.

B) Simplifying exponentiation mod k : explain why the 2nd equality holds:

$$\overbrace{507}^{m}{}^{123} \pmod{\overbrace{14}^{k}} = (\overbrace{\underset{k}{14} \times \underset{q}{36} + \underset{r}{3}}^{\text{division by } 14 = k})^{123} \pmod{14} = 3^{123} \pmod{14}$$

$$(kq+r)^{123} = \underbrace{\cdots + 123\, kq \cdot r^{122}}_{\text{all terms have factor of } k \Rightarrow \text{ vanish when do mod } k} + r^{123}$$

Hence state a preliminary step to make exp mod k more efficient.

b^n mod k alg: first replace b by b mod k. then do usual fast exponentiation mod k.

C) Use Euclid's algorithm to compute $g = \gcd(2261, 1275)$ by hand:

$$\begin{array}{r} 2261 \\ -\ 1275 \\ \hline 986 \end{array} \qquad g = \gcd(1275, 986) \qquad \begin{array}{r} 1275 \\ -\ 986 \\ \hline 289 \end{array}$$

$g = \gcd(986, 289)$ $\quad 3 \times 289 = 867$ $\qquad \begin{array}{r} 986 \\ -\ 867 \\ \hline 119 \end{array}$ $\qquad \gcd(289, 119)$ $\quad 2 \times 119 = 238$

$\gcd(119, 51) = \gcd(51, 17) = \underline{17}$

D) Factor 8051 [Hint: how close is it to 8100?]

$$8051 = 8100 - 49 = 90^2 - 7^2 = (90+7)(90-7) = 97 \cdot 83$$

This will be basis of Fermat's method.

(they are both prime).