Lecture 12: Divisibility — Math 345

Tuesday, October 12, 2010 — Jim Fowler

Textbook

This lecture discusses section 4 of the textbook.

Homework

The homework is due Thursday, October 14, 2010.

From Section 4 of the textbook, do exercises 13, 14, and 15.

divisibility

d and x integers. d divides x means that there exists an integer k so that $x = kd$.

what about zero?

examples

a divides a.

If a divides b and a divides c, then a divides $b + c$.

If a divides b and a divides c, then a divides $b - c$.

If a divides b or a divides c, then a divides bc.

congruences

a, b, m integers. $a \equiv b \pmod{m}$ means m divides $a - b$.

prove it is an equivalence relation.

some amusing calculations

$2^n \equiv 2 \pmod{n}$ for which values of n?

$2^3 \equiv \mathbf{2} \pmod{3}$
$2^4 \equiv 0 \pmod{4}$
$2^5 \equiv \mathbf{2} \pmod{5}$
$2^6 \equiv 4 \pmod{6}$
$2^7 \equiv \mathbf{2} \pmod{7}$
$2^8 \equiv 0 \pmod{8}$
$2^9 \equiv 8 \pmod{9}$
$2^{10} \equiv 4 \pmod{10}$
$2^{11} \equiv \mathbf{2} \pmod{11}$
$2^{12} \equiv 4 \pmod{12}$
$2^{13} \equiv \mathbf{2} \pmod{13}$
$2^{14} \equiv 4 \pmod{14}$
$2^{15} \equiv 8 \pmod{15}$
$2^{16} \equiv 0 \pmod{16}$
$2^{17} \equiv \mathbf{2} \pmod{17}$
$2^{18} \equiv 10 \pmod{18}$
$2^{19} \equiv \mathbf{2} \pmod{19}$
$2^{20} \equiv 16 \pmod{20}$
$2^{21} \equiv 8 \pmod{21}$
$2^{22} \equiv 4 \pmod{22}$
$2^{23} \equiv \mathbf{2} \pmod{23}$
$2^{24} \equiv 16 \pmod{24}$
$2^{25} \equiv 7 \pmod{25}$
$2^{26} \equiv 4 \pmod{26}$
$2^{27} \equiv 26 \pmod{27}$
$2^{28} \equiv 16 \pmod{28}$
$2^{29} \equiv \mathbf{2} \pmod{29}$
$2^{30} \equiv 4 \pmod{30}$
$2^{31} \equiv \mathbf{2} \pmod{31}$
$2^{32} \equiv 0 \pmod{32}$
$2^{33} \equiv 8 \pmod{33}$
$2^{34} \equiv 4 \pmod{34}$
$2^{35} \equiv 18 \pmod{35}$
$2^{36} \equiv 28 \pmod{36}$
$2^{37} \equiv \mathbf{2} \pmod{37}$
$2^{38} \equiv 4 \pmod{38}$
$2^{39} \equiv 8 \pmod{39}$
$2^{40} \equiv 16 \pmod{40}$
$2^{41} \equiv \mathbf{2} \pmod{41}$
$2^{42} \equiv 22 \pmod{42}$
$2^{43} \equiv \mathbf{2} \pmod{43}$
$2^{44} \equiv 16 \pmod{44}$
$2^{45} \equiv 17 \pmod{45}$
$2^{46} \equiv 4 \pmod{46}$
$2^{47} \equiv \mathbf{2} \pmod{47}$
$2^{48} \equiv 16 \pmod{48}$
$2^{49} \equiv 30 \pmod{49}$
$2^{50} \equiv 24 \pmod{50}$
$2^{51} \equiv 8 \pmod{51}$
$2^{52} \equiv 16 \pmod{52}$
$2^{53} \equiv \mathbf{2} \pmod{53}$
$2^{54} \equiv 28 \pmod{54}$
$2^{55} \equiv 43 \pmod{55}$
$2^{56} \equiv 32 \pmod{56}$
$2^{57} \equiv 8 \pmod{57}$
$2^{58} \equiv 4 \pmod{58}$
$2^{59} \equiv \mathbf{2} \pmod{59}$
$2^{60} \equiv 16 \pmod{60}$
$2^{61} \equiv \mathbf{2} \pmod{61}$
$2^{62} \equiv 4 \pmod{62}$
$2^{63} \equiv 8 \pmod{63}$
$2^{64} \equiv 0 \pmod{64}$
$2^{65} \equiv 32 \pmod{65}$
$2^{66} \equiv 64 \pmod{66}$
$2^{67} \equiv \mathbf{2} \pmod{67}$
$2^{68} \equiv 16 \pmod{68}$
$2^{69} \equiv 8 \pmod{69}$
$2^{70} \equiv 44 \pmod{70}$
$2^{71} \equiv \mathbf{2} \pmod{71}$
$2^{72} \equiv 64 \pmod{72}$
$2^{73} \equiv \mathbf{2} \pmod{73}$
$2^{74} \equiv 4 \pmod{74}$
$2^{75} \equiv 68 \pmod{75}$
$2^{76} \equiv 16 \pmod{76}$
$2^{77} \equiv 18 \pmod{77}$
$2^{78} \equiv 64 \pmod{78}$
$2^{79} \equiv \mathbf{2} \pmod{79}$
$2^{80} \equiv 16 \pmod{80}$
$2^{81} \equiv 80 \pmod{81}$
$2^{82} \equiv 4 \pmod{82}$
$2^{83} \equiv \mathbf{2} \pmod{83}$
$2^{84} \equiv 64 \pmod{84}$
$2^{85} \equiv 32 \pmod{85}$
$2^{86} \equiv 4 \pmod{86}$
$2^{87} \equiv 8 \pmod{87}$
$2^{88} \equiv 80 \pmod{88}$
$2^{89} \equiv \mathbf{2} \pmod{89}$
$2^{90} \equiv 64 \pmod{90}$
$2^{91} \equiv 37 \pmod{91}$
$2^{92} \equiv 16 \pmod{92}$
$2^{93} \equiv 8 \pmod{93}$
$2^{94} \equiv 4 \pmod{94}$
$2^{95} \equiv 13 \pmod{95}$
$2^{96} \equiv 64 \pmod{96}$
$2^{97} \equiv \mathbf{2} \pmod{97}$
$2^{98} \equiv 18 \pmod{98}$
$2^{99} \equiv 17 \pmod{99}$
$2^{100} \equiv 76 \pmod{100}$
$2^{101} \equiv \mathbf{2} \pmod{101}$
$2^{102} \equiv 64 \pmod{102}$
$2^{103} \equiv \mathbf{2} \pmod{103}$
$2^{104} \equiv 48 \pmod{104}$

pseudoprimes

$2^{341} = 44794894843556084211148845611368885562432909944692990697999782019275837423603218907$
which is congruent to 2 modulo 341. But 341 is not prime, being 11 times 31.

what is going on?

$$
\begin{aligned}
2^{341} &\equiv 2 \pmod{341} \\
2^{561} &\equiv 2 \pmod{561} \\
2^{645} &\equiv 2 \pmod{645} \\
2^{1105} &\equiv 2 \pmod{1105} \\
2^{1387} &\equiv 2 \pmod{1387} \\
2^{1729} &\equiv 2 \pmod{1729} \\
2^{1905} &\equiv 2 \pmod{1905} \\
2^{2047} &\equiv 2 \pmod{2047} \\
2^{2465} &\equiv 2 \pmod{2465} \\
2^{2701} &\equiv 2 \pmod{2701} \\
2^{2821} &\equiv 2 \pmod{2821} \\
2^{3277} &\equiv 2 \pmod{3277} \\
2^{4033} &\equiv 2 \pmod{4033} \\
2^{4369} &\equiv 2 \pmod{4369} \\
2^{4371} &\equiv 2 \pmod{4371} \\
2^{4681} &\equiv 2 \pmod{4681}
\end{aligned}
$$

necklace proof

Theorem: If p is prime, then $2^p \equiv 2 \pmod{p}$.

proof: want to show $2^p - 2$ is divisible by p.

$2^p - 2$ = number of strings of two symbols, where both symbols appear.

cyclic shifts split the remaining necklaces into groups of p (because p is prime).