Boston University — Summer I 2009

Number Theory — Kalin Kostadinov

Quiz V

student:
06/16/2009

Question 1: Realign the columns and fill in the five blanks:

Mathematician	Theorem	Example
0) __	I There exist infinitely many _ _	A: $13 = 2^2 + 3^2$
1) Euclid	II $(a, b) = 1 \Rightarrow \exists\, x, y : ax + by = 1$	B $2, 3, 5, 7, \cdots$
2) Fermat	III $(a, n) = 1 \Rightarrow a^{\phi(n)} \equiv 1 \pmod{n}$	C: $(5, 7) = 1$ and $5 \cdot 3 + 7 \cdot (-2) = 1$
3) Euler	IV Let p be a prime $p \equiv$ _ _ then p is a sum of ___	D: $x^2 \equiv 5(modp)$ has solution if and only if $x^2 \equiv p(mod5)$ has (p is an arbitrary odd prime)
4) Diophantus	V Law of Quadratic Reciprocity	E: _ _

0 - -
1 - -
2 - -
3 - -
4 - -

Question 2: Solve the congruences:

$$19x \equiv 13 \pmod{26} \qquad\qquad x^2 + 5x \equiv 7 \pmod{1}1$$

Question 3: For the following two statements, first give a restatement, than give the contrary statement.
Example: Let $a, b \in \mathbb{N}$. If a and b are relatively prime, then the arithmetic progression $a, a+b, a+2b\dots$ contains infinitely many prime numbers.
In other words, if the arithmetic progression $a, a+b, a+2b\dots$ contains only finitely many prime numbers, then a and b are not relatively prime.
Indeed, assume the contrary, that there exists a pair of relatively prime numbers a and b, such that the arithmetic progression $a, a+b, a+2b\dots$ contains only finitely many prime numbers.

Fact: Let $a, p \in \mathbb{N}$. If p is prime, and a is relatively prime with p, then $a^{p-1} \equiv 1 \pmod{p}$. Equivalently,...

Indeed, assume the contrary ...

Fact: If every proper divisor of an integer is even, then the integer must be a power of 2. Equivalently, ...

Indeed, assume the contrary...

Question 4: Only one of the three Linear Diophantine equations has a solution. Use the Euclid algorithm to find which one, and then to solve it.
A) $679x + 315y = 5$.
B) $679x + 315y = 6$.
C) $679x + 315y = 7$.