Boston University	Number Theory
Summer I 2009	Kalin Kostadinov

Quiz IV

student:
06/09/2009

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

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

0 -V- D (Like this)
1 - -
2 - -
3 - -
4 - -

Question 2: We know that every natural number is the sum of at most 4 squares of natural numbers, and for some numbers 3 squares will not suffice. The number 7 is the smallest one of the latter type, which number is the second smallest?

Question 3: Give an example of a four-digit number that is not sum of two squares. Give an example of a second four digit number that is sum of two squares.

Question 4: What is the result of running the following pseudo-code:

```
M:= 12,N:= 30; - - user input
WHILE(N>0) DO - - start a cycle
    IF(N>M)
        THEN TEMP=M;M=N;N=TEMP; - - flip M and N
    END-IF;
    TEMP=M;
    M=N;
    N=TEMP-N;
END-OF-WHILE; - - end of cycle
PRINT(M);
```

Question 5: Use Fermat's Little Theorem and the Chinese Reminder Theorem, or Euler's theorem to compute $1234567^{2345} \pmod{15}$.