NAME (printed neatly)_____ QUIZ#7 GRADE _____

Directions for taking quizzes: the same as in the previous quizzes.

1. A word has been broken into blocks of two letters and converted to two-digit numbers using the correspondence

$$a \mapsto 4,\ b \mapsto 2, d \mapsto 0, e \mapsto 3,\ k \mapsto 8, n \mapsto 1,\ o \mapsto 9, l \mapsto 5,\ r \mapsto 7$$

The blocks are then encoded using the RSA public key system with base 55 and the exponent 27. The coded message is 04/07. Find the word which was coded (explain each step of your decoding process).

2. Assume that on the set $\mathbb{P}$ of all positive integers the following relation $\mathbb{R}$ is given: aRb if and only of a and b are coprime. Decide whether R is reflexive, symmetric, antisymmetric or transitive. Justify your answers.

1. $n = 55 = 5 \times 11 \Rightarrow \varphi(n) = (5-1)(11-1) = 40$

Find x such that $27x + 40y = 1$ for some integer y using the matrix form of the Euclidean algorithm:

$$\begin{pmatrix} 1 & 0 & 27 \\ 0 & 1 & 40 \end{pmatrix} \xrightarrow{R_2 \to R_2 - R_1} \begin{pmatrix} 1 & 0 & 27 \\ -1 & 1 & 13 \end{pmatrix} \xrightarrow{R_1 \to R_1 - 2R_2} \begin{pmatrix} 3 & -2 & 1 \\ -1 & 1 & 13 \end{pmatrix} \Rightarrow$$

$x = 3$

(Check $27 \times 3 - 40 \times 2 = 81 - 80 = 1$)

i) To decode the first block find $4^3 \bmod 55$: $4^3 = 64 \equiv 9 \bmod 55 \Rightarrow$ it results in 09 → do

ii) To decode the second block find $7^3 \bmod 55$: $7^3 = 343 \equiv 13 \bmod 55 \Rightarrow$ it results in 13 → ne

$\Rightarrow$ The answer is **done**

2. reflexive: no, e.g. 2 is not coprime to itself

symmetric: yes if $\gcd(a,b) = 1$ then $\gcd(b,a) = 1$

antisymmetric: no (If the relation is symmetric and non empty then it is not antisymmetric)

transitive: no example $a = 21$, $b = 5$, $c = 7$

$\gcd(a,b) = 1$, $\gcd(b,c) = 1$ But $\gcd(21,7) = 7$, i.e. aRb and bRc but a is not related to c.