Some number theory and combinatorics questions

January 12, 2012

(1) Find r and s such that $gcd(119, 315) = 119r + 315s$,

(2) Find an integer x such that

$$202x \equiv 33 \ (mod\ 431)$$

(3) Determine by computing a Jacobi/Legendre symbol if

$$x^2 + 14x \equiv 194 \ (mod\ 389)$$

has a solution (note 389 is prime).

(4) Alice and Bob wish to set up a Diffie-Hellman public key cryptosystem. Their first step is to agree on a public modulus $p = 17$ and the primitive root $a = 11$. Alice publishes her public key as the number 5 (remember it is the primitive root raised to her secret key) and Bob publishes 14 as his public key. What is the common key between Alice and Bob ($a^{\text{secret key for Alice}\cdot\text{secret key for Bob}}$). The powers of 3 mod 17 are

$$3^1 = 3, 3^2 = 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1$$

(5) Alice and Bob send a message with a Diffie-Hellman with public modulus

$$p = 98345729843759028374509238745902387450923874509234750932847 9$$

They choose a primitive root of 13 and then Alice picks her secret key of 105 and sends to Bob her public key of

$$7590123799793888980623742091231109558884128058200714289738 69$$

(why did she send this number?). Bob picks his secret key as 3053 and sends to Alice his public key of

$$4300101360087454209452487525021821004354297800411177801783 71$$

(again, why did he send this number?). Alice then sends to Bob the encrypted message C as

$$8007267173621560305724973151475634869424016654306912841542 91$$

where $C \equiv M + K \ (mod\ p)$ and M is the message and K is their common key. Recover the message and the common key.