(i) The integers a and $n>1$ satisfy $a^{n-1} \equiv 1 \pmod{n}$ but $a^m \not\equiv 1 \pmod{n}$ for each divisor m of $n-1$, other than itself. Prove that n is a prime.

(ii) Show that if n is not a Pseudoprime to base bb', $\gcd(b, b') = 1$, then it is not a Pseudoprime to either base b or b'.

(iii) Prove that 1105 and 1729 are Carmichael numbers.

(iv) Find the smallest positive integer k s.t $a^k \equiv 1 \pmod{756}$ for every integer $(a, 756) = 1$.

(v) Someone wishes to send Jim, a message, let $N = 49601$ and $s = 247$.

Code : Use 00 for a blank
01 for a
02 for b
⋮

(Eg. No $\equiv$ 1415)

Suppose the message is M.

let $E \equiv M^s \pmod{N}$ where $0 < E < N$.

Then M is your actual message, & E is the encrypted message.

Suppose Jim knows the prime factorization of N. (You can use a computer to find the prime factorization of 49601)

(a) Using the Euclidean algorithm, help Jim find the private key t s.t

$st \equiv 1 \pmod{\phi(N)}$

(b) Compute the encrypted message E (for the message $M = $ "No") and then verify your work by decoding E.

(vi) Let n be a positive integer. Prove

$$\left(\sum_{m|n} d(m)\right)^2 = \sum_{m|n} d^3(m), \quad \text{where}$$

$$d(n) = \sum_{m|n} 1$$

(vii) Let $N = 3^{10!} - 1$. Show that $N \equiv 0 \bmod 125$. State any named-theorem you are using.

(viii) Let g be a primitive root modulo 29.

(a) How many primitive roots are there modulo 29.

(b) Find a primitive root g modulo 29.

(c) Use g mod 29 to find all the primitive roots modulo 29.

(d)

(ix) Show that the hyperbola

$$C: x^2 - 67y^2 = 31$$ has no integral points.

(x) How many primitive roots are there modulo 12^{100}?

(xi) Which of the following can be written as a sum of two squares? A sum of 3 squares? 4 squares?

(a) 39420
(b) 55555
(c) 34578
(d) 12!
(e) A no. of the form p^2+2, p prime