M 343 L 55540 Final

name:
ssn:
signature:

Do three out of the four questions below and please indicate here which questions you chose:

1. If $n = 77$ and $e = 17$ are the public modulus and encryption exponent, respectively, of a user of the RSA cryptosystem, find the decryption exponent. Find the message whose encryption by the above parameters is 20.

2. Describe the Pollard $p-1$ factoring algorithm and explain why it works.

3. Let E be the elliptic curve $y^2 = x^3 + 1$ modulo 17 and consider the point $P = (2, 3)$ on it. Find $2P$ and $3P$.

4. Let p be a prime number and m an integer. Show that $(1+p)^m \equiv 1+mp \pmod{p^2}$. Explain how this could be used to solve the discrete logarithm problem modulo p^2 if you can solve the discrete logarithm problem modulo p.