

Due: Thursday May 3, 5pm.

1. If a and b are odd numbers show that $a^2 + b^2$ is not a square number.
2. Show that any number of the form $n^5 - n$ is divisible by 30.
3. Show that $\sum_{d|n} \phi(d) = n$.
4. By adapting the Euclidean Algorithm proof for unique factorisation of numbers, state and prove a unique factorisation theorem for polynomials.
5. Suppose that Alice has an RSA encryption scheme with primes p and q and public key e . Describe a procedure whereby she can send a message to Bob, together with a signature that Bob can verify comes from Alice, which cannot be faked without knowledge of Alice's private key.
6. (i) Suppose f_1, \dots, f_k are polynomials with integer coefficients in the variables x_1, \dots, x_n , all having constant term 0. Let d_i be the total degree of f_i for $1 \leq i \leq k$ and suppose $d_1 + \dots + d_k < n$. Let p be a prime. Show that one can choose x_1, \dots, x_n not all congruent to 0 mod p so that $f_i(x_1, \dots, x_n) \equiv 0 \pmod{p}$ for $1 \leq i \leq k$. (Adapt the proof of Chevalley's Theorem.)
(ii) Suppose we have linear forms $L_i(x_1, \dots, x_n) = \sum_{j=1}^n c_{ij}x_j$ for $1 \leq i \leq k$, p is prime and $n > k(p-1)$. By considering the polynomials $f_i(y_1, \dots, y_n) = L_i(y_1^{p-1}, \dots, y_n^{p-1})$ show that one can set each x_i equal to 0 or 1, and not all of them equal to 0, so that $L_i(x_1, \dots, x_n) \equiv 0 \pmod{p}$ for $1 \leq i \leq k$.
(iii) Suppose p is prime and (a_1, \dots, a_{2p-1}) is an integer sequence. By considering $L_1(x_1, \dots, x_{2p-1}) = \sum_{i=1}^n x_i$ and $L_2(x_1, \dots, x_{2p-1}) = \sum_{i=1}^n a_i x_i$ show that there is a subsequence $(a_{i_1}, \dots, a_{i_p})$ of length p so that $a_{i_1} + \dots + a_{i_p} \equiv 0 \pmod{p}$.
(iv) Suppose n is a number and (a_1, \dots, a_{2n-1}) is an integer sequence. Show that there is a subsequence $(a_{i_1}, \dots, a_{i_n})$ of length n so that $a_{i_1} + \dots + a_{i_n} \equiv 0 \pmod{n}$. Is this necessarily true if we start with a shorter sequence?