EE720: Problems set 2.1: CRT, cyclic groups, finite fields

Sept 6, 2020

1. Find q-adic expansions: of 34787, 55833, (34787)(55833) for $q = 25, 101$ on calculator.

   Hint: See the expansion formula and algorithm in Theorem 1.3.3 in Buchmann.

2. Show how you can find the multiple base expansion of numbers. (We can call such expansion polyadic). For $b_1 = 2, b_2 = 3$ such an expansion represents a number a in the form
$$a = a_{00} + a_{10}2 + a_{01}3 + a_{11}2.3 + a_{21}2^2.3 + a_{12}2.3^2 + a_{22}2^2.3^2 + \ldots$$
   What is the largest power of the base required given the number a? Develop a method of high school multiplication and division with remainder in terms of polyadic expansion. Compute expansions of numbers in problem 1 above in bases $2, 3$.

   Hint: Outside syllabus. Think on your own. Look at wiki page on polyadic representation of numbers.

3. Compute $\gcd(139024789, 93278890)$ using calculator and find one extended Euclidean representation of the gcd.

   Hint: Use the extended Euclidean algorithm discussed in class.

4. Let d be $\gcd(a, b)$ and u, v satisfy $d = au + bv$. Find all solutions x, y of the identity $d = ax + by$ in terms of a, b, u, v, d.

   Hint: Consider any other pair of solutions $d = ax' + by'$. Subtract the two identities and solve.

5. For a natural number n and a prime p, order of p in n denoted $\mathrm{ord}_p(n)$ is the power of p that appears in prime factorization of n. Find $\mathrm{ord}_2(2816)$, $\mathrm{ord}_7(2222574487)$, $\mathrm{ord}_p(46375)$ for $p = 3, 5, 7$.

   Hint: Use order computation algorithm discussed in class.

6. Order of an element in a group. For groups $\mathbb{Z}_n^*$ this is the multiplicative order. Use the algorithm discussed in class to find orders of at one of the primes not dividing $\phi(n)$ in $\mathbb{Z}_n^*$ for $n = 256, 1000, 2816$. Then check your answer using the sage function for multiplicative order.

   Hint: Already given.

7. Find at least one primitive element modulo $p = 23, 29, 41, 43$. Find all primitive roots of $p = 11, 17, 23$. How many primitive roots modulo p are there for a prime p? Compute number of primitive roots of $p = 41, 57, 97, 101, 1001$. How many primitive roots are there in $\mathbb{Z}_n^*$ for $n = 23 * 29$.

   Hint: by trial, choose random integer $< p$ and find order. You are likely to succeed with probability 0.6.

8. Let C_n denote a cyclic group of order n. Write the lattice of all subgroups of C_{100}, C_{36}, C_{12}.

   Hint: Every divisor of n has a cyclic subgroup.

9. Solve following congruences (or explain why solutions dont exist) using Euler's theorem (i.e. not using extended Euclidean algorithm).

   (a) $x = 37 \mod 43$, $x = 22 \mod 49$, $x = 18 \mod 71$.

   (b) $x = 133 \mod 451$, $x = 237 \mod 697$.

   (c) $x = 5 \mod 9$, $x = 6 \mod 10$, $x = 7 \mod 11$.

   Hint: In CRT formula inverse modulo n can be obtained by Euler's formula.

10. Find following powers by fast exponentiation using binary expansion and also using CRT whenever possible 1) $17^{183} \mod 256$, 2) $2^{477} \mod 1000$, $11^{507} \mod 1237$.

    Hint: Already given.

11. Construct irreducible polynomials of degree $2, 3, 5$, over $GF(p)$ for $p = 2, 3, 5, 7, 11$. Construct extension fields $\mathbb{F}_q$ for $q = p^n$ for $p = 2, 3$, $n = 2$ and write their multiplication table in terms of a root θ of the chosen irreducible polynomial. Find one primitive element of $\mathbb{F}_q$ for these fields.

    Hint: Search irreducible polynomials of required degree by constructing from degree 2 then using these for degree 3 etc. Field tables are witten by the rule $f(\theta) = 0$ where f is the generating irreducible polynomial.

12. Write the lattice diagram of all subfields of $\mathbb{F}_{2^{16}}$, $\mathbb{F}_{3^8}$. Write the lattice diagram of all subgroups of the cyclic group of units of these fields. Are these same? Justify.

13. Find primitive elements of the fields $\mathbb{F}_{2^4}$, $\mathbb{F}_{3^3}$ by representing them in a polynomial basis of root of an irreducible polynomial.

    Hint: First construct irreducible polynomials to represent the fields. Search for orders of roots of generating polynomials. The root θ should have orders equal to $\mathbb{F}_q^*$.

14. Represent finite fields $\mathbb{F}_{2^m}$ for $m = 3, 5, 7$ by a polynomial basis $\{1, \theta, \dots, \theta^{m-1}\}$. Find order of θ in each of these fields. Show that the polynomial $X^8 + X^4 + X^3 + X + 1$ is irreducible over $\mathbb{F}_2$. Find order of a root of this polynomial. Is this polynomial primitive?

    Hint: Straightforward.