M E T U
Department of Mathematics

Elementary Number Theory I Final	
Code : *Math 365* Acad. Year : *2014* Semester : *Fall* Instructor : *Küçüksakallı* Date : *January 5, 2014* Time : *13:30* Duration : 150 *minutes*	Last Name : Name : Student No. : Signature : 7 QUESTIONS ON 4 PAGES 100 TOTAL POINTS

1	2	3	4	5	6	7		

1. (24pts) For each of the following statements determine if it is true or false. If it is true, explain briefly. If it is false, give a counter example.

(a) If a is an integer then $6|a(a^2+11)$.

Solution: TRUE. The integer a is congruent $0,1,2,3,4$ or 5 modulo 6. In either case $a(a^2+11) \equiv 0 \pmod 6$.

(b) If $\gcd(a,b)=1$, then $\gcd(a+2b, 2a+b)=1$.

Solution: FALSE. If $a=b=1$, then $\gcd(a+2b, 2a+b)=3$.

(c) Any positive integer of the form $3k+2$ has a prime divisor of the same form.

Solution: TRUE. Let p be a prime divisor of $3k+2$. Then $p \neq 3$. Thus $p \equiv 1, 2 \pmod 3$. If all the prime divisors of $3k+2$ are of the form $3m+1$ then so is $3k+2$ which is impossible.

(d) If $\gcd(m,n) > 2$, then the system $x \equiv 1 \pmod n, x \equiv -1 \pmod m$ has no solutions.

Solution: TRUE. Let $d = \gcd(m,n)$ and assume to the contrary x is such a solution. Then $x \equiv \pm 1 \pmod d$. This is possible only if $d=1$ or $d=2$.

(e) If $a^p \equiv a \pmod p$ for all integers a, then p is a prime number.

Solution: FALSE. There are Carmichael numbers.

(f) If r is a primitive root of a prime p then r is a primitive root of $2p^k$ for any $k \geq 1$.

Solution: FALSE. The prime 5 has a primitive root $r=2$ whereas $r=2$ is not a primitive root of 10.

2. (12pts) Find integers x, y, z such that $77x + 91y + 143z = 1$.

Solution: Applying the Euclidean algorithm to the pair $(11, 13)$, it can be found that $6 \cdot 11 - 5 \cdot 13 = 1$. Thus $6 \cdot 77 - 5 \cdot 91 = 7$. Applying the Euclidean algorithm to the pair $(7, 143)$, it can be found that $41 \cdot 7 - 2 \cdot 143 = 1$. Therefore $41(6 \cdot 77 - 5 \cdot 91) - 2 \cdot 143 = 1$. Thus we can choose $x = 246, y = -205$ and $z = -2$.

3. (16pts) Define $f(n) = \gcd(n, 200)$ and $F(n) = \sum_{d|n} f(d)$.

(a) Show that f is multiplicative.

Solution: Let $n = n_1 n_2$ with $\gcd(n_1, n_2) = 1$. It follows that $\gcd(n, 200) = \gcd(n_1, 200)\gcd(n_2, 200)$. Thus $f(n) = f(n_1)f(n_2)$.

(b) Is F multiplicative? Compute $F(9000)$.

Solution: Since f is multiplicative, so is F. We have $F(9000) = F(2^3)F(3^2)F(5^3)$. Thus $F(9000) = (1 + 2 + 4 + 8)(1 + 1 + 1)(1 + 5 + 25 + 25)$.

(c) If $N = 10^k + 1$ for some integer $k \geq 1$, then show that $\sum_{d|N} \mu(d) F\left(\frac{N}{d}\right) = 1$.

Solution: By Mobius inversion formula the sum is equal to $f(N)$. It is easy to see that $f(N) = 1$ since N is not divisible by 2 and 5.

4. (12pts) Let $n = pq$ where p and q are twin primes, i.e. $|p - q| = 2$.

(a) Show that there exists an integer r which is a primitive root of both p and q.

Solution: Let r_1 be a primitive root of p and r_2 be a primitive root of q. By Chinese remainder theorem, there exists an integer r such that $r \equiv r_1 \pmod{p}$ and $r \equiv r_2 \pmod{q}$.

(b) Show that the order of r modulo n is $\phi(n)/2$.

Solution: Since p and q are twin primes, they are congruent to 1 and 3 modulo 4 respectively without loss of generality. Thus $\gcd(p - 1, q - 1) = 2$ and as a result $\operatorname{lcm}(p - 1, q - 1) = (p - 1)(q - 1)/2 = \phi(n)/2$. It follows that $r^{\phi(n)/2} \equiv 1 \pmod{n}$. We also need to see that $k = \phi(n)/2$ is the smallest exponent so that $r^k \equiv 1 \pmod{n}$. Since $r^k \equiv 1 \pmod{n}$, we have $r^k \equiv 1 \pmod{p}$ as well. Thus $p - 1$ divides k. Similarly $q - 1$ divides k. As a result $\operatorname{lcm}(p - 1, q - 1)$ divides k. This finishes the proof.

5. (12pts) Consider the integer $N = n^4 + n^3 + n^2 + n + 1$ with $n \geq 1$. If p is a prime divisor of N, then show that $p = 5$ or $p \equiv 1 \pmod{10}$.

Solution: Let p be a prime divisor of N. Then $N \equiv 0 \pmod{p}$. It follows that $n^5 - 1 \equiv 0 \pmod{p}$. The order of n modulo p can be either 1 or 5. The first case is possible only if $p = 5$. If p is not 5, then $5 | \phi(p) = p - 1$. Thus p is of the form $5k + 1$. Since p is prime k must be even and we have $p \equiv 1 \pmod{10}$.

6. (12pts) Let $p \geq 5$ be an odd prime and let r be a primitive root of p.

(a) Show that r^2 is not a primitive root of p.

Solution: Since p is an odd prime $(p-1)/2$ is an integer. It follows that $(r^2)^{(p-1)/2} \equiv 1 \pmod{p}$. Thus the order of r^2 is less than or equal to $\phi(p)/2 = (p-1)/2$. Thus r^2 is not a primitive root of p.

(b) Show that r^3 is a primitive root of p if and only if $p \equiv 2 \pmod{3}$.

Solution: The order of r^3 modulo p is equal to $\phi(p)/\gcd(\phi(p), 3)$. This order is equal to $\phi(p)$ if and only if $\gcd(p-1, 3) = 1$. This is possible if and only if $p \equiv 2 \pmod{3}$

7. (12pts) Let $p \geq 7$ be a prime. Note that $p = 20q + r$ for some $0 \leq r < 20$ by the division algorithm. Show that the equation $x^2 + 5 \equiv 0 \pmod{p}$ has a solution if and only if $0 < r < 10$.

Solution: Recall that $(\frac{-1}{p}) = 1$ if and only if $p \equiv 1 \pmod{4}$. We also have $(\frac{5}{p}) = 1$ if and only if $p \equiv \pm 1 \pmod{5}$ by the quadratic reciprocity law. Combining these facts together by Chinese remainder theorem, we see that $(\frac{-5}{p}) = 1$ if and only if $r \equiv 1, 3, 7, 9 \pmod{20}$. This finishes the proof.