Name ________________________ Math 332 Prelim 2

November 14, 2001 Instructor: Lawren Smithline

Solve the following problems. Justify your answers. Closed calculators, closed notes, closed book. Please state clearly any result you use from class or the book. (You don't need to prove them again here.) All problems have equal weight. **55 minutes**.

1. a. Given that 3 is a primitive element modulo 19, the (incomplete) table of indices:

$a =$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
ind $a =$	0		1	14	4											W		

compute the smallest positive value for W where $W =$ **ind** 16
and find the smallest positive value for x which solves $5^x \equiv 16$ (modulo 19).

b. Determine whether 2 is a primitive element modulo 241. (You may assume 241 is prime.)

2. a. Compute the Legendre symbol $\left(\dfrac{37}{241}\right)$. As ever, state clearly any result you use.

2. b. Let p be prime. Prove that $(n^2-2)(n^2-5)(n^2-40)$ is divisible by p for infinitely many values of n.

3. a. Express $\frac{31}{11}$ as a continued fraction.

b. Let $\alpha = \langle 1, \overline{1,2} \rangle = 1 + \frac{1}{1+}\frac{1}{2+}\frac{1}{1+}\frac{1}{2+}\cdots$.

Find the convergent $\frac{p}{q}$ to α with the smallest denominator such that $|\frac{p}{q} - \alpha| < \frac{1}{500}$.
(Remember to justify that q is the smallest.)

Solutions

1. a. $16 = 4^2$, so **ind** $16 \equiv 2 \cdot$**ind** $4 \equiv 28$ modulo $\phi(19)$. 19 is prime, so $\phi(19) = 18$. The smallest positive integer congruent to 28 modulo 18 is $W = 10$.

From the table, the index of 5 is 4, so using indices, x is the smallest positive solution to $4x \equiv 10 \equiv 28$ modulo 18. Divide everything including the modulus by 2 to get: $2x \equiv 14$ modulo 9. The solution is $x = 7$.

1. b. The residue 2 is a primitive element modulo 241 if and only if its order is 240. The prime divisors of 240 are 2, 3, 5. So if 2 is a perfect square, cube, or fifth power, then it is NOT a primitive element.

241 is 1 modulo 8, so 2 is a quadratic residue. So 2 is NOT a primitive element.

Coincidentally, $243 = 3^5$, so 2 is a fifth power residue also, and still not primitive.

2. a. 241 is 1 modulo 8, so it is 1 modulo 4. By the law of Quadratic Reciprocity, $(\frac{37}{241}) = (\frac{241}{37})$. Reduce 241 modulo 19, and notice $37 \equiv 1$ modulo 4. So $(\frac{241}{37}) = (\frac{37}{19})$. Reduce 37 modulo 19 to -1. The prime 19 is congruent to 3 modulo 4, so $(\frac{-1}{19}) = -1$. Thus, $\left(\frac{37}{241}\right) = -1$.

2. b. Let p be the given prime. Let $f(n) = (n^2-2)(n^2-5)(n^2-40)$. If $p \mid f(n)$, then $p \mid f(n+tp)$ for any integer t. So for each p, once we find one solution, we know there are infinitely many.

If $p = 2$ or $p = 5$ then $p \mid f(0)$. For other primes: notice that $(\frac{10}{p}) = (\frac{40}{p})$ and $(\frac{2}{p})(\frac{5}{p}) = (\frac{10}{p})$. In this last equation, not every term can be -1. So at least one of 2, 5, and 40 is a quadratic residue modulo p. So there is n such that $p \mid f(n)$.

3. a. $\frac{31}{11} = 2 + \frac{1}{11/9} = 2 + \frac{1}{1+\frac{1}{9/2}} = 2 + \frac{1}{1+\frac{1}{4+\frac{1}{2}}}$.

3. b. The first few convergents to α are:

a_n		1	1	2	1	2	1	2
p_n	1	1	2	5	7	19	26	71
q_n	0	1	1	3	4	11	15	41.

Recall $\left|\frac{p_n}{q_n} - \alpha\right| < \frac{1}{q_n q_{n+1}}$.

Notice that $15 \cdot 41 = 615 > 500$, so $|\frac{26}{15} - \alpha| < \frac{1}{500}$.

The previous even convergents are all further away from α than $\frac{71}{41}$, and $|\frac{19}{11} - \frac{71}{41}| \geq 1/450$.

The previous odd convergents are all further away from α than $\frac{26}{15}$ and $|\frac{7}{4} - \frac{26}{15}| \geq 1/60$.