Solution

Math 445

Exam 1

Show all work. How you get your answer is just as important, if not more important, than the answer itself. If you think it, write it!

1. (25 pts.) Find the period of the repeating decimal expansion of 1/41 (by computing the order of the appropriate integer modulo the appropriate integer).

Find $\mathrm{ord}_{41}(10)$! $\quad 41-1=\phi(41)=40$ so $\mathrm{ord}_{41}(10) \mid 40=2^3\cdot 5$

so $\mathrm{ord}_{41}(10)=1,2,4,5,8,10,20,$ or $\underline{40}$.

$10^1=10\equiv_{41}10$

$10^2=100=82+18\equiv_{41}18$

$10^4\equiv_{41}18^2=324=41\cdot 7+37\equiv_{41}-4$

$10^8\equiv_{41}(-4)^2=16$

$10^5\equiv_{41}37\cdot 10=370=369+1\equiv_{41}1$

$$\begin{array}{r} 18 \\ \times 18 \\ \hline 144 \\ 18 \\ \hline 324 \\ -287 \\ \hline 37 \end{array}$$

so $\mathrm{ord}_{41}(10)=\underline{\underline{5}}$

so the period of $\frac{1}{41}$ is $\underline{\underline{5}}$.

2. (25 pts.) Show that if $ab \equiv 1 \pmod n$, then $ord_n(a) = ord_n(b)$.

$k = ord_n(a) \quad m = ord_n(b)$, so

$a^k \underset{n}{\equiv} 1$, $b^m \underset{n}{\equiv} 1$.

$(ab) \underset{n}{\equiv} 1 \implies (ab)^k \underset{n}{\equiv} 1$, but

$(ab)^k \underset{n}{\equiv} a^k b^k \underset{n}{\equiv} 1 \cdot b^k \underset{n}{\equiv} b^k$ so $b^k \underset{n}{\equiv} 1$, so $m | k$.

__But__ $(ab)^m \underset{n}{\equiv} a^m b^m \equiv a^m \cdot 1 \equiv a^m$ so $a^m \underset{n}{\equiv} 1$, so $k | m$

$\underset{n}{\equiv}$
1

__So__ $k | m$ and $m | k$, so $k = \pm m$. Since both are ≥ 1,

we have $ord_n(a) = k = m = ord_n(b)$.

3. (25 pts.) Find the number of (incongruent, modulo 21) solutions to the congruence equation

$$x^5 \equiv 4 \pmod{21}$$

$21 = 3 \cdot 7$, so look at solutions mod 3 and mod 7

$x^5 \underset{3}{\equiv} 4$

$3-1=2 \quad (5,2)=1$

Check $4^{2/1} \underset{3}{\equiv} 1$?

Yes by ~~E~~ Fermat's Little Theorem, since $(4,3)=1$

So $x^5 \underset{3}{\equiv} 4$ has $(5,2)=1$ soln.

$x^5 \underset{7}{\equiv} 4$

$7-1=6 \quad (5,6)=1$

Check $4^{6/1} \underset{7}{\equiv} 1$?

Yes, by Fermat's Little Theorem, since $(4,7)=1$

So $x^5 \underset{7}{\equiv} 4$ has $(5,6)=1$ soln.

So $x^5 \underset{21}{\equiv} 4$ has $1 \cdot 1 = 1$ solution.

4. (25 pts.) Show that if an integer n can be expressed as the sum of the squares of two *rational* numbers

$$n = (\frac{a}{b})^2 + (\frac{c}{d})^2 ,$$

then n can be expressed as the sum of the squares of two *integers*.

(Hint: Not directly! Show that n has the correct prime factorization....)

$$n = \frac{a^2}{b^2} + \frac{c^2}{d^2} \implies n = \frac{a^2d^2 + c^2b^2}{b^2d^2}$$

$\implies nb^2d^2 = (ad)^2 + (bc)^2$ is a sum of squares.

So the prime factors of nb^2d^2 which are $\equiv 3 \pmod 4$ all appear with even exponent.

But then the same is true for n, since if n had a prime factor $p \equiv 3 \pmod 4$ with $p^{2k+1} \mid n$, $p^{2k+2} \nmid n$ then for k_1, k_2 the exponents of p in b and d, we have

$p^{2(k+k_1+k_2)+1} \mid nb^2d^2$ but $p^{2(k+k_1+k_2)+2} \nmid nb^2d^2$

so p has odd exponent in pb^2d^2, a contradiction

So all primes of the form $p \equiv 3 \pmod 4$ have even exponent in n, so n can be expressed as the sum of two squares.