

#1-15a.

$$p \equiv 1 \pmod{4} \Leftrightarrow p = 4m + 1$$

r is a primitive root mod p

$$\text{so } \text{ord}_p r = p - 1 = 4m$$

Why is $-r$ a primitive root?

$$-r = r \cdot (-1). \text{ Since } r \text{ is a}$$

quadratic non-residue mod p

(it's a primitive root), $-1 = \left(\frac{r}{p}\right)$

$$\equiv r^{\frac{p-1}{2}} = r^{2m} \equiv -1 \pmod{p}$$

$$\text{so } -r \equiv r^1 \cdot r^{2m} = r^{2m+1} \pmod{p}.$$

Since $\text{gcd}(2m+1, 4m) = 1$

it follows that r^{2m+1} is also a p-root.

13b. A simpler question

$$p \equiv 3 \pmod{4} \Rightarrow p = 4m + 3$$

$$\frac{p-1}{2} = 2m+1$$

Again, r is a quadratic non-residue,

$$\text{so } -1 = \left(\frac{r}{p}\right) = r^{\frac{p-1}{2}} = r^{2m+1} \equiv -1 \pmod{p}.$$

$$\text{Thus } -r = r(-1) = r^{1+(2m+1)}$$

$$\equiv r^{2m+2}$$

$$\text{and } \text{ord}_p r^{2m+2} = \frac{\text{ord}_p r}{\text{gcd}(\text{ord}_p r, 2m+2)}$$

$$= \frac{4m+2}{\text{gcd}(2m+2, 4m+2)}$$

$$\text{gcd}(2m+2, 4m+2)$$

Clearly $2 \mid 2m+1, 2 \mid 4m+2$, so

$$\text{gcd}(2m+2, 4m+2) = 2 \text{gcd}(m+1, 2m+1)$$

$$\text{Since } 1 = 2(m+1) + (-1)(2m+1),$$

$$\text{gcd}(2m+2, 4m+2) = 2 \cdot 1 = 2$$

$$\text{and } \text{ord}_p -r = \text{ord}_p r^{2m+2}$$

$$= \frac{4m+2}{2} = 2m+1 = \frac{p-1}{2}$$

#2-50e

$$7x^5 \equiv 2 \pmod{17}$$

The table says that 3

is a primitive root mod 17

$$3^0 \equiv 1 \quad 3^4 \equiv 13 \quad 3^8 \equiv 16 \quad 3^{12} \equiv 4$$

$$3^1 \equiv 3 \quad 3^5 \equiv 5 \quad 3^9 \equiv 14 \quad 3^{13} \equiv 12$$

$$3^2 \equiv 9 \quad 3^6 \equiv 15 \quad 3^{10} \equiv 8 \quad 3^{14} \equiv 2$$

$$3^3 \equiv 10 \quad 3^7 \equiv 11 \quad 3^{11} \equiv 7 \quad 3^{15} \equiv 6$$

$$\text{so } 3^{11} \cdot x^5 \equiv 3^{14} \pmod{17}$$

$$\text{let } x \equiv 3^n$$

$$3^{11} \cdot 3^{5n} \equiv 3^{14} \pmod{17}$$

$$\text{or } 3^{5n-3} \equiv 1 \pmod{17}$$

$$\Leftrightarrow 5n \equiv 3 \pmod{16} \quad (16 = \phi(17))$$

$$\text{now } 5 \cdot 13 = 65 \equiv 1 \pmod{16}$$

$$\text{(or } 5 \cdot (-3) = -15, \text{ but } 13 \equiv -3 \pmod{16})$$

$$\text{so } 13 \cdot 5n \equiv 13 \cdot 3 \pmod{16}$$

$$65n \equiv 39 \pmod{16}$$

$$n \equiv 7 \pmod{16}$$

$$\text{and } x \equiv 3^n \equiv 3^7 \equiv 11 \pmod{17}$$

#3 37 Theorem 5.21

We know that $x^n \equiv a \pmod{m}$

has $\begin{cases} \text{gcd}(n, \phi(m)) \\ 0 \end{cases}$ solutions if

$$a^{\frac{\phi(m)}{\text{gcd}(n, \phi(m))}} \equiv 1 \pmod{m}$$

Here, $\text{gcd}(a, m) = 1$ and $m = 1, 2, 4, p^n$ or $2 \cdot p^n$

p is a prime ($m = p$ is ok) $\text{gcd}(a, m) = 1$.

If $p \equiv 1 \pmod{6}$ and $n = 3$, then

$$m = p = 6k + 1$$

$$\phi(m) = 6k \quad n = 3, \text{gcd}(n, \phi(m)) =$$

$$\text{gcd}(3, 6k) = 3, \text{ so there are}$$

3 or 0 solutions

If $p \equiv 5 \pmod{6}$ and $n = 3$

$$\text{then } p = m = 6k + 5 \quad \phi(m) = 6k + 4$$

$$\text{and } \text{gcd}(n, \phi(m)) = \text{gcd}(3, 6k + 4) = 1$$

In this case $a^{\frac{\phi(m)}{\text{gcd}(n, \phi(m))}} \equiv 1 \pmod{m}$ always

Math 455
HW 10
Due 11/28/07

4a $4x + 10y = 21$
 $\Leftrightarrow 2x + 5y = 21$ $\text{gcd}(2, 5) = 1$
 One solution is $x_0 = 8$ $y_0 = 1$
 So all integer solutions are given by
 a. $x = 8 + 5t$, $y = 1 - 2t$, $t \in \mathbb{Z}$
 b. These are positive if
 $8 + 5t \geq 0$ $t \geq -1.6$
 $1 - 2t \geq 0$ $t \leq .5$
 i.e., for $t = -1, 0, 1$
 $(x, y) = (3, 3)$ or $(8, 1)$

5. $x^2 + y^2 = z^2$
 primitive $453 = m^2 - n^2$
 $y = 2mn$
 $z = m^2 + n^2$

$\text{gcd}(m, n) = 1$ one of (m, n) even, one odd.

$453 = 453 \cdot 1 = (m+n)(m-n)$ is

one choice $\begin{matrix} m+n = 453 \\ m-n = 1 \end{matrix} \Rightarrow$

$m = 227$ $n = 226$ will work

so $y = 2 \cdot 226 \cdot 227 (= 102604)$

$z = 226^2 + 227^2 (= 102605)$

primitive $2008 = 2mn$
 $y = m^2 - n^2$
 $z = m^2 + n^2$

(it doesn't matter what you call x & y , but $m^2 - n^2$ is odd + $2mn$ is even.

$mn = 1004$ Again, we want

$\text{gcd}(m, n) = 1$ and one of (m, n) even,

the other odd. Try $m = 251$, $n = 4$

This gives $y = 251^2 - 4^2 (= 62985)$

$z = 251^2 + 4^2 (= 63017)$.

There are no other solutions here, because 251 is prime.

6. $x^2 + 5y^2 = z^2$

Recall: $a^2 \equiv 0 \pmod{3}$ if $3|a$
 and $a^2 \equiv 1 \pmod{3}$ if $3 \nmid a$.

Thus, if $x^2 + 5y^2 = z^2$

Then $x^2 + 5y^2 \equiv z^2 \pmod{3}$.

If $3|x$ we're done. If $3|y$ we're

done. Suppose neither x nor y is divisible by 3. Then $x^2 \equiv 1 \pmod{3}$

and $y^2 \equiv 1 \pmod{3}$, so $x^2 + 5y^2 \equiv 1 + 5$

$\equiv 0 \equiv z^2 \pmod{3}$, so $3|z^2$ and $3|z$.

Thus 3 has to divide at least one of $\{x, y, z\}$.

7. Note that $2^2 + 5 \cdot 1^2 = 4 + 5 = 9 = 3^2$
 and 7 does not divide 1, 2 or 3.

8 Solution 1.

$400x^2 + 53y^2 = 400z^2$

$\Rightarrow 400 | 53y^2$ and $\text{gcd}(53, 400) = 1$

$\Rightarrow 400 | y^2 \Rightarrow 20 | y$. Write $y = 20u$

$400x^2 + 53 \cdot 400u^2 = 400z^2$

$x^2 + 53u^2 = z^2$

$53u^2 = z^2 - x^2 = (z+x)(z-x)$

One way to do this is to take

$u = 1$, $z+x = 53$, $z-x = 1$

so $u = 1$, $z = 27$, $x = 26$ $y = 20$

$400 \cdot 26^2 + 53 \cdot 20^2 = 400 \cdot 27^2$

Solution 2. Divide by $400z^2$

$\left(\frac{x}{z}\right)^2 + \frac{53}{400} \left(\frac{y}{z}\right)^2 = 1$

The equation

$u^2 + \frac{53}{400} v^2 = 1$

is an ellipse and $(1, 0)$ is on it

As before, we write

$$u = 1 + t$$

$$v = 0 + mt \quad \text{for fixed } m$$

and solve for

$$(1+t)^2 + \frac{53}{400} m^2 t^2 = 1$$

$$2t + \left(1 + \frac{53}{400} m^2\right) t^2 = 0$$

$$t = -\frac{2}{1 + \frac{53}{400} m^2}$$

If we take $m=20$, to make the denominator nice, from example

$$t = \frac{-2}{1+53} = -\frac{1}{27}$$

$$u = 1 - \frac{1}{27} \quad v = 0 + \frac{-20}{27}$$

$$u = \frac{26}{27} \quad v = -\frac{20}{27}$$

$$\frac{11}{x} \quad \frac{11}{z}$$

We get $x=26$ $y=-20$ $z=27$

make $y=+20$ to get positive results.

9a. Sure.

$$x = m^2 - n^2$$

$$y = 2mn$$

$$z = m^2 + n^2$$

$$x+y+z = 2m^2 + 2mn = 2m(m+n)$$

$$xy = (m^2 - n^2) 2mn = 2m(m+n) \cdot n(n-m)$$

9b. No. $2^5 = 32 \equiv 1 \pmod{31}$

so $\text{ord}_{31} 2 \leq 5$

(it actually equals 5).

9c. Nope. $141^2 = z^2 - x^2 = (z-x)(z+x)$

$$\text{Let } z+x = 141^2 \quad z = \frac{141^2 + 1}{2}$$

$$z-x = 1 \quad x = \frac{141^2 - 1}{2}$$

($x=9940$, $z=9941$)

10. If w, x, y, z are all odd,

$$\text{Then } w^2 \equiv x^2 \equiv y^2 \equiv z^2 \equiv 1 \pmod{4}$$

$$\text{so } w^2 + x^2 + y^2 + z^2 \equiv 3 \not\equiv 1 \pmod{4},$$

hence at least one of $\{x, y, z, w\}$ is even, so $2 \mid wxyz$.

If $3 \nmid w, x, y, z$, Then $w^2 \equiv x^2 \equiv y^2 \equiv z^2 \equiv 1$

$\pmod{3}$, so $1+1+1 \equiv 1 \pmod{3}$, another

contradiction, so $3 \mid wxyz$ and

$$\text{so } 2 \cdot 3 = 6 \mid wxyz$$

11. We have $\phi(p) = p-1$. If g^3 is not a primitive root, Then $\text{gcd}(3, p-1) > 1 \Rightarrow$

$$\text{gcd}(3, p-1) = 3 \Rightarrow p \equiv 1 \pmod{3}$$

If g^5 is not a primitive root, Then $\text{gcd}(5, p-1) > 1$

$$\Rightarrow \text{gcd}(5, p-1) = 5 \Rightarrow p \equiv 1 \pmod{5}$$

Since p is odd, $p \equiv 1 \pmod{2}$, so

$2, 3, 5$ all divide $p-1$, hence $30 \mid p-1$

$$\text{or } p \equiv 1 \pmod{30}.$$

12. $2007 = 2 \cdot 1003 + 1$

$$1003 = 2 \cdot 501 + 1$$

$$501 = 2 \cdot 250 + 1$$

$$250 = 2 \cdot 125 + 0$$

$$125 = 2 \cdot 62 + 1$$

$$62 = 2 \cdot 31 + 0$$

$$31 = 2 \cdot 15 + 1$$

$$15 = 2 \cdot 7 + 1$$

$$7 = 2 \cdot 3 + 1$$

$$3 = 2 \cdot 1 + 1$$

$$1 = 2 \cdot 0 + 1$$

Reading up: $[2007]_2 = 11111010111$

check $2007 = 2^{10} + 2^9 + 2^8 + 2^7 + 2^6 + 2^4 + 2^3 + 2^1$

$$= 1024 + 512 + 256 + 128 + 64 + 16 + 4 + 2 + 1$$

$$= 2007 \quad \checkmark$$

$$\begin{aligned}
2007 &= 3 \cdot 669 + 0 \\
669 &= 3 \cdot 223 + 0 \\
223 &= 3 \cdot 74 + 1 \\
74 &= 3 \cdot 24 + 2 \\
24 &= 3 \cdot 8 + 0 \\
8 &= 3 \cdot 2 + 2 \\
2 &= 3 \cdot 0 + 2
\end{aligned}$$

$$\begin{aligned}
\text{so } [2007]_3 &= 2202100 \\
\text{Check } 2 \cdot 3^6 + 2 \cdot 3^5 + 2 \cdot 3^3 + 3^2 \\
&= 2 \cdot 729 + 2 \cdot 243 + 2 \cdot 27 + 9 \\
&= 1458 + 486 + 54 + 9 = 2007
\end{aligned}$$

$$\begin{aligned}
2007 &= 5 \cdot 401 + 2 \\
401 &= 5 \cdot 80 + 1 \\
80 &= 5 \cdot 16 + 0 \\
16 &= 5 \cdot 3 + 1 \\
3 &= 5 \cdot 0 + 3
\end{aligned}$$

$$\begin{aligned}
\text{so } [2007]_5 &= 31012 \\
3 \cdot 5^4 + 5^3 + 5 + 2 \\
&= 3 \cdot 625 + 125 + 5 + 2 = 2007.
\end{aligned}$$

13. We need to find
 $v_2(2007!)$
 $v_3(2007!)$
 $v_5(2007!)$.

Using The formula from class
and the handouts

$$v_p(n!) = \frac{n - \text{sum of base } p \text{ digits of } n}{p-1}$$

$$\text{so } v_2(2007!) = \frac{2007 - 9}{1} = 1998$$

$$v_3(2007!) = \frac{2007 - (2+2+2+1)}{3-1} = \frac{2007-7}{2} = 1000$$

$$v_5(2007!) = \frac{2007 - (2+1+4+3)}{5-1} = \frac{2007-7}{4} = 1000$$

$$6! = 720 = 2^4 \cdot 3^2 \cdot 5$$

$$\text{so } (6!)^r = 2^{4r} \cdot 3^{2r} \cdot 5^r$$

$$\text{ord}(6!)^r \mid 2007!$$

if and only if

$$4r \leq v_2(2007!) = 1998$$

$$2r \leq v_3(2007!) = 1000$$

$$r \leq v_5(2007!) = 500$$

$$\text{or } r \leq 499.5$$

$$r \leq 500$$

$$r \leq 500$$

The largest r that does this is 499.

Fibonacci summary:

$$F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2}, n \geq 2.$$

n	0	1	2	3	4	5	6	7	8	9
F _n	0	1	1	2	3	5	8	13	21	34

$$\phi = \frac{1+\sqrt{5}}{2} \approx 1.618 \dots$$

$$\bar{\phi} = \frac{1-\sqrt{5}}{2} \approx -0.618 \dots$$

$\phi, \bar{\phi}$ are roots of $x^2 - x - 1 = 0$

$$F_n = \frac{1}{\sqrt{5}} (\phi^n - \bar{\phi}^n)$$

F_n facts:

$$(i) 2 \mid F_n \iff 3 \mid n$$

$$(ii) 3 \mid F_n \iff 4 \mid n$$

(iii)

$$F_{m+n+1} = F_{m+1}F_{n+1} + F_mF_n$$

(iv)

$$F_{2n} = F_n(F_{n-1} + F_{n+1})$$

$$F_{2n+1} = F_n^2 + F_{n+1}^2$$

$$(v) \sum_{n=0}^{\infty} F_n x^n = \frac{x}{1-x-x^2} \quad |x| < \frac{1}{\phi}$$

#1. The key here is The formula

$$\text{ord}_m(a^k) = \frac{\text{ord}_m a}{\text{gcd}(k, \text{ord}_m a)}$$

and the formula $-r = (-1) \cdot T$.

And: $a^n \equiv 1 \pmod{m}$

$\Rightarrow \text{ord}_m a \mid n$, not equality

#2 Mostly right.

#3. Don't be afraid of a problem because it looks hard; it might not be.

#4 Lots of different (x_0, y_0)
The most common one was algorithmic.
 $4x + 10y = 42 \Leftrightarrow 2x + 5y = 21$
and $\text{gcd}(2, 5) = 1 \Rightarrow -2 \cdot 2 + 5 \cdot 1 = 1$
so $2(-42) + 5(21) = 21$. Or, you could find $(3, 3)$ or $(8, 1)$ by inspection. Any valid method is ok online.

#5 A typo led some of you to seek all primitive solutions

$$x^2 + y^2 = z^2$$

x odd $x = n^2 - m^2$ $\text{gcd}(m, n) = 1$
 y even $\rightarrow y = 2mn$ one of (m, n) even
 z odd $z = n^2 + m^2$ one odd.

$$\begin{aligned} \text{For } 453 \quad 453 &= n^2 - m^2 \\ &= (n+m)(n-m) \\ &= 453 \cdot 1 \quad (a) \\ &= 151 \cdot 3 \quad (b) \end{aligned}$$

(a) $\Rightarrow n=227, m=226$, solution assigned

(b) $\Rightarrow n=77, m=74, x=11405, y=11396$.

For 2008 $2008^2 + y^2 = z^2$ and primitive, we have to have

$$\begin{aligned} 2008 &= 2mn \\ y &= n^2 - m^2 \\ z &= n^2 + m^2 \end{aligned}$$

I was wrong on my notes:

$$2008 = 2mn$$

$$\Rightarrow 1004 = mn$$

$$1004 = 4 \cdot 251, 251 \text{ prime.}$$

so $n=251, m=4$ as in notes 1

$$a^n = 1004, m=1, y=1008015, z=1008017.$$

Math 453
HW 10
More Conns

#6, 7 Done in class

#8 Other popular solutions:
 $(47, 400, 153), (347, 800, 453), (5299, 100, 5301)$

#9 b. One person astutely noted that $(\frac{2}{31}) = 1$ because $31 \equiv 7 \pmod{8}$, so 2 is a quadratic residue and not a p.r. But I think it's easier to look at 25.

#9 c. A non-primitive example is $(3 \cdot 47)^2 + (4 \cdot 47)^2 = (5 \cdot 47)^2$

#10 Done in class

#11 This is a simpler version of #1
See comment for #3

#12, 13 Clearly, the most popular problems

The point here was that

$$L_p(n!) = \frac{n - \text{sum of digits in } n \text{ base } p}{p-1}$$

Remember - if you have any questions on this, or any other course material, please bring them to class.

You can also send me an email before Monday and I will cover the topic without you having to ask in public!