Midterm #2: practice

MATH 311 — Intro to Number Theory
Midterm: Tuesday, Nov 12

Please print your name:

Bonus challenge. Let me know about any typos you spot in the posted solutions (or lecture sketches). Any typo, that is not yet fixed by the time you send it to me, is worth a bonus point.

Problem 1.

(a) Determine the number of invertible residues modulo 116.

(b) Determine the (multiplicative) order of 2 modulo 11.

(c) Is 2 a primitive root modulo 11?

(d) For which a is 2^a a primitive root modulo 11?

(e) List all primitive roots modulo 11.

(f) Suppose $x \pmod{n}$ has (multiplicative) order k. What is the order of x^a?

(g) What is the number of primitive roots modulo 101?

Solution.

(a) The number of invertible residues modulo 116 is $\phi(116) = \phi(4)\phi(29) = 2 \cdot 28 = 56$.

(b) The order of 2 must divide $\phi(11) = 10$. The only possibilities therefore are $1, 2, 5, 10$.

Since $2^2 = 4 \not\equiv 1$, $2^5 = 32 \equiv -1 \not\equiv 1 \pmod{11}$, we conclude that the order of 2 is 10.

(c) Since the order of $2 \pmod{11}$ equals $\phi(11)$, 2 is a primitive root modulo 11.

(d) 2^a is a primitive root modulo 11 if and only if $\gcd(a, 10) = 1$.

(e) Hence, the primitive roots modulo 11 are $2^1 = 2$, $2^3 = 8$, $2^7 \equiv 7$, $2^9 \equiv 6$.

(f) x^a has order $\frac{k}{\gcd(k, a)}$.

(g) The number of primitive roots modulo 101 is $\phi(\phi(101)) = \phi(100) = 40$. □

Problem 2.

(a) Find the smallest positive integer x simultaneously solving the four congruences:

$x \equiv 1 \pmod{3}$, $x \equiv 2 \pmod{4}$, $x \equiv 3 \pmod{5}$, $x \equiv 4 \pmod{11}$.

(b) What is the next largest solution x to the above congruences?

(c) Solve $x \equiv 1 \pmod{3}$, $x \equiv 2 \pmod{4}$, $2x \equiv 3 \pmod{5}$, $3x \equiv 4 \pmod{11}$.

(d) Find the smallest integer $a > 2$ such that $2|a$, $3|(a+1)$, $4|(a+2)$ and $5|(a+3)$.

Solution.

(a) Since $3\cdot 4\cdot 5\cdot 11 = 660$, by the Chinese remainder theorem, the general solution is

$$x \equiv 1\cdot 220\cdot \underbrace{220_{\text{mod}3}^{-1}}_{1} + 2\cdot 165\cdot \underbrace{165_{\text{mod}4}^{-1}}_{1} + 3\cdot 132\cdot \underbrace{132_{\text{mod}5}^{-1}}_{3} + 4\cdot 60\cdot \underbrace{60_{\text{mod}11}^{-1}}_{-2}$$
$$\equiv 220 + 330 + 1188 - 480 = 1258 \equiv 598 \equiv -62 \pmod{660}.$$

The smallest positive integer solution therefore is $x = 598$.

(b) The next largest solution x to the above congruences is $x = 598 + 660 = 1258$.

(c) $2x \equiv 3 \pmod 5$ has the unique solution $x \equiv 2^{-1}\cdot 3 \equiv 3\cdot 3 \equiv -1 \pmod 5$.

$3x \equiv 4 \pmod{11}$ has the unique solution $x \equiv 3^{-1}\cdot 4 \equiv 4\cdot 4 \equiv 5 \pmod{11}$.

Our simplified task therefore is to solve $x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 4$, $x \equiv -1 \pmod 5$, $x \equiv 5 \pmod{11}$. We reuse the previous part to produce the solution

$$x \equiv 1\cdot 220\cdot \underbrace{220_{\text{mod}3}^{-1}}_{1} + 2\cdot 165\cdot \underbrace{165_{\text{mod}4}^{-1}}_{1} - 1\cdot 132\cdot \underbrace{132_{\text{mod}5}^{-1}}_{3} + 5\cdot 60\cdot \underbrace{60_{\text{mod}11}^{-1}}_{-2}$$
$$\equiv 220 + 330 - 396 - 600 = -446 \equiv 214 \pmod{660}.$$

(d) This is the same as solving $a \equiv 0 \pmod 2$, $a \equiv -1 \pmod 3$, $a \equiv -2 \pmod 4$, $a \equiv -3 \pmod 5$. Notice that we can't apply the Chinese remainder theorem directly, because 2 and 4 are not coprime.

However, if $a \equiv -2 \pmod 4$ then, automatically, $a \equiv 0 \pmod 2$. So, we can drop the latter congruence and only look for solutions of $a \equiv -1 \pmod 3$, $a \equiv -2 \pmod 4$, $a \equiv -3 \pmod 5$.

By the Chinese remainder theorem (since $3, 4, 5$ are pairwise coprime), there is a unique solution a modulo $3\cdot 4\cdot 5 = 60$. Note that $a = 2$ is such a solution. Hence, the next smallest solution is $a = 62$.

[Don't worry if you didn't see that $a = 2$ is a solution. You can find it by going through the same kind of computations as in the previous parts.] □

Problem 3.

(a) Using the Chinese remainder theorem, determine all solutions to $x^2 \equiv 4 \pmod{55}$.

(b) Using the Chinese remainder theorem, determine all solutions to $x^2 \equiv 1 \pmod{105}$.

(c) How many solutions does the congruence $x^2 \equiv 1 \pmod N$ have for $N = 210$? Modulo $N = 1995$?

Solution.

(a) By the Chinese remainder theorem (CRT):

$$\begin{aligned} & x^2 \equiv 4 \pmod{55} \\ \Longleftrightarrow\ & x^2 \equiv 4 \pmod 5 \text{ and } x^2 \equiv 4 \pmod{11} \\ \Longleftrightarrow\ & x \equiv \pm 2 \pmod 5 \text{ and } x \equiv \pm 2 \pmod{11} \end{aligned}$$

The two obvious solutions modulo 55 are ± 2. To get one of the two additional solutions, we solve $x \equiv 2 \pmod 5$, $x \equiv -2 \pmod{11}$. [Then the other additional solution is the negative of that.]

$$x \equiv 2\cdot 11\cdot \underbrace{11_{\text{mod}5}^{-1}}_{1} - 2\cdot 5\cdot \underbrace{5_{\text{mod}11}^{-1}}_{-2} \equiv 22 + 20 \equiv 42 \equiv -13 \pmod{55}$$

Hence, the solutions are $x \equiv \pm 2 \pmod{55}$ and $x \equiv \pm 13 \pmod{55}$.

(b) Note that $105 = 3 \cdot 5 \cdot 7$. By the CRT, x is a solution to $x^2 \equiv 1 \pmod{105}$ if and only if x is a solution to the three congruences

$$x^2 \equiv 1 \pmod{3}, \quad x^2 \equiv 1 \pmod{5}, \quad x^2 \equiv 1 \pmod{7}.$$

Since $3, 5, 7$ are primes each of these only has the obvious solutions $x \equiv \pm 1$. Using the CRT, these combine in $2 \cdot 2 \cdot 2 = 8$ different ways to a solution modulo 105. For instance, one the 8 possibilities is

$$\begin{aligned} & x \equiv -1 \pmod{3}, \quad x \equiv 1 \pmod{5}, \quad x \equiv -1 \pmod{7} \\ \Longleftrightarrow \quad & x \equiv -1 \cdot 5 \cdot 7 \cdot \underbrace{[(5 \cdot 7)^{-1}_{\bmod 3}]}_{2} + 1 \cdot 3 \cdot 7 \cdot \underbrace{[(3 \cdot 7)^{-1}_{\bmod 5}]}_{1} - 1 \cdot 3 \cdot 5 \cdot \underbrace{[(3 \cdot 5)^{-1}_{\bmod 7}]}_{1} = -70 + 21 - 15 \equiv 41 \pmod{105}. \end{aligned}$$

Corresponding to it is the negative case $x \equiv 1 \pmod{3}$, $x \equiv -1 \pmod{5}$, $x \equiv 1 \pmod{7}$ which is equivalent to $x \equiv -41 \pmod{105}$.

Likewise, we determine all 8 solutions as follows:

$$\begin{array}{llll} x \equiv 1 \pmod{3}, & x \equiv 1 \pmod{5}, & x \equiv 1 \pmod{7} & \Longleftrightarrow \; x \equiv 1 \pmod{105} \\ x \equiv 1 \pmod{3}, & x \equiv 1 \pmod{5}, & x \equiv -1 \pmod{7} & \Longleftrightarrow \; x \equiv -29 \pmod{105} \\ x \equiv 1 \pmod{3}, & x \equiv -1 \pmod{5}, & x \equiv 1 \pmod{7} & \Longleftrightarrow \; x \equiv -41 \pmod{105} \\ x \equiv 1 \pmod{3}, & x \equiv -1 \pmod{5}, & x \equiv -1 \pmod{7} & \Longleftrightarrow \; x \equiv 34 \pmod{105} \\ x \equiv -1 \pmod{3}, & x \equiv 1 \pmod{5}, & x \equiv 1 \pmod{7} & \Longleftrightarrow \; x \equiv -34 \pmod{105} \\ x \equiv -1 \pmod{3}, & x \equiv 1 \pmod{5}, & x \equiv -1 \pmod{7} & \Longleftrightarrow \; x \equiv 41 \pmod{105} \\ x \equiv -1 \pmod{3}, & x \equiv -1 \pmod{5}, & x \equiv 1 \pmod{7} & \Longleftrightarrow \; x \equiv 29 \pmod{105} \\ x \equiv -1 \pmod{3}, & x \equiv -1 \pmod{5}, & x \equiv -1 \pmod{7} & \Longleftrightarrow \; x \equiv -1 \pmod{105} \end{array}$$

Note that, because each case has a negative, we only need to compute 4 of these 8 cases (of which one is the trivial solution).

In summary, $x^2 \equiv 1 \pmod{105}$ has exactly the 8 solutions $x \equiv \pm 1, \pm 29, \pm 34, \pm 41$ modulo 105.

(c) Since $210 = 2 \cdot 3 \cdot 5 \cdot 7$, we can again use the Chinese remainder theorem and argue as in the previous case. There is just one difference: the congruence $x^2 \equiv 1 \pmod{2}$ only has 1 solution (because $1 \equiv -1 \pmod{2}$). Hence, we find that the congruence $x^2 \equiv 1 \pmod{210}$ has $1 \cdot 2 \cdot 2 \cdot 2 = 8$ solutions.

On the other hand, since $1995 = 3 \cdot 5 \cdot 7 \cdot 19$, the congruence $x^2 \equiv 1 \pmod{1995}$ will have $2 \cdot 2 \cdot 2 \cdot 2 = 16$ solutions. □

Problem 4.

(a) What are the last two (decimal) digits of 3^{4488}?

(b) Determine $137^{738} \pmod{63}$.

Solution.

(a) We need to determine $3^{4488} \pmod{100}$. Since $\gcd(3, 100) = 1$ and $\phi(100) = \phi(4)\phi(25) = 2 \cdot 20 = 40$ and $4488 \equiv 8 \pmod{40}$, we have $3^{4488} \equiv 3^8 \pmod{100}$. We compute $3^2 = 9$, $3^4 = 81 \equiv -19$, $3^8 \equiv (-19)^2 \equiv 61 \pmod{100}$ and conclude that $3^{4488} \equiv 61 \pmod{100}$. This means that the last two (decimal) digits of 3^{4488} are 61.

(b) Clearly, $137^{738} \equiv 11^{738} \pmod{63}$. Since $\gcd(11, 63) = 1$ as well as $\phi(63) = \phi(3^2)\phi(7) = (3^2 - 3^1) \cdot 6 = 36$ and $738 \equiv 18 \pmod{36}$, we have $137^{738} \equiv 11^{18} \pmod{63}$.

Binary exponentiation: $11^2 = 121 \equiv -5$, $11^4 \equiv 25$, $11^8 \equiv 625 \equiv -5$, $11^{16} \equiv 25 \pmod{63}$.

Hence, $137^{738} \equiv 11^2 \cdot 11^{16} \equiv -5 \cdot 25 \equiv 1 \pmod{63}$.

Comment. Our calculation shows that $11^{18} \equiv 1 \pmod{63}$. Indeed, the order of $11 \pmod{63}$ is equal to 18 (which divides $\phi(63) = 36$). □

Problem 5. For unknown reasons, the high priest of number theory has banned usage of the Euclidean algorithm. With the help of the Chinese remainder theorem, determine the modular inverse of 149 modulo 666.

Solution. Note that $666 = 2\cdot 9\cdot 37$. We first compute 149^{-1} modulo each of $2, 9, 37$. That's super easy: $149^{-1} \equiv 1^{-1} \equiv 1 \pmod{2}$, $149^{-1} \equiv 5^{-1} \equiv 2 \pmod{9}$ and $149^{-1} \equiv 1^{-1} \equiv 1 \pmod{37}$.

By the Chinese remainder theorem,

$$149^{-1} \equiv 1\cdot 9\cdot 37\cdot \underbrace{[(9\cdot 37)^{-1}_{\bmod 2}]}_{1} + 2\cdot 2\cdot 37\cdot \underbrace{[(2\cdot 37)^{-1}_{\bmod 9}]}_{5} + 1\cdot 2\cdot 9\cdot \underbrace{[(2\cdot 9)^{-1}_{\bmod 37}]}_{-2} \equiv 333 + 740 - 36 \equiv 1037 \equiv 371 \pmod{666}. \quad \square$$

Problem 6. Compute $7^{111} \pmod{90}$ in the following three different ways:

(a) Directly, using binary exponentiation.

(b) With the help of Euler's theorem.

(c) With the help of the Chinese remainder theorem (as well as Euler's theorem).

Solution.

(a) Modulo 90, we have $7^2 = 49$, $7^4 = 49^2 \equiv 61$, $7^8 \equiv 61^2 \equiv 31$, $7^{16} \equiv 31^2 \equiv 61$, $7^{32} \equiv 31$, $7^{64} \equiv 61$.

Therefore, $7^{111} = 7^{64}\cdot 7^{32}\cdot 7^8\cdot 7^4\cdot 7^2\cdot 7 \equiv 61\cdot 31\cdot 31\cdot 61\cdot 49\cdot 7 \equiv 73 \pmod{90}$.

(b) Since $90 = 2\cdot 3^2\cdot 5$, we find $\phi(90) = 90\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 24$ so that Euler's theorem tells us that $7^{24} \equiv 1 \pmod{90}$. Since $111 \equiv 15 \pmod{24}$, we have $7^{111} \equiv 7^{15} = 7^8\cdot 7^4\cdot 7^2\cdot 7 \equiv 31\cdot 61\cdot 49\cdot 7 \equiv 73 \pmod{90}$.

(c) Notice that $90 = 2\cdot 3^2\cdot 5$, where $2, 9, 5$ are pairwise coprime.

Computing 7^{111} modulo each of $2, 9, 5$ is much easier (note that $\phi(9) = 9\left(1-\frac{1}{3}\right) = 6$ so that, by Euler's theorem $7^6 \equiv 1 \pmod{9}$; on the other hand, $7^4 \equiv 1 \pmod{5}$):

$$7^{111} \equiv 1^{111} \equiv 1 \pmod{2}, \quad 7^{111} \equiv 7^3 \equiv (-2)^3 \equiv 1 \pmod{9}, \quad 7^{111} \equiv 7^3 \equiv 2^3 \equiv 3 \pmod{5}.$$

By the Chinese remainder theorem,

$$7^{111} \equiv 1\cdot 9\cdot 5\cdot \underbrace{[(9\cdot 5)^{-1}_{\bmod 2}]}_{1} + 1\cdot 2\cdot 5\cdot \underbrace{[(2\cdot 5)^{-1}_{\bmod 9}]}_{1} + 3\cdot 2\cdot 9\cdot \underbrace{[(2\cdot 9)^{-1}_{\bmod 5}]}_{2} \equiv 45 + 10 + 108 \equiv 73 \pmod{90}.$$

Comment. While this might seem like the most involved approach (it certainly requires the most expertise), observe that the actual computations are much simpler than in the other cases (because we are operating modulo very small numbers). □

Problem 7. Note that $323 = 17\cdot 19$.

(a) Modulo 323, what do we learn from Euler's theorem?

(b) Using the Chinese remainder theorem, show that $x^{144} \equiv 1 \pmod{323}$ for all x coprime to 323. (Compare!)

Solution.

(a) Since $\phi(323) = \phi(17)\phi(19) = 16\cdot 18 = 288$, we learn that $x^{288} \equiv 1 \pmod{323}$ for all x that are coprime to 323.

(b) By the Chinese remainder theorem, the congruence $x^{144} \equiv 1 \pmod{323}$ is true for all x coprime to 323 (or, equivalently, all x coprime to both 17 and 19) if and only if the two congruences $x^{144} \equiv 1 \pmod{17}$ and $x^{144} \equiv 1 \pmod{19}$ are true for all such x.

By Fermat's little theorem, we have $x^{16} \equiv 1 \pmod{17}$ and hence $x^{144} \equiv (x^{16})^9 \equiv 1 \pmod{17}$. Likewise, $x^{18} \equiv 1 \pmod{19}$ implies that $x^{144} \equiv (x^{18})^8 \equiv 1 \pmod{19}$.

Comparison. If $x^{144} \equiv 1 \pmod{323}$, then $x^{288} = (x^{144})^2 \equiv 1 \pmod{323}$. This means that Euler's theorem is weaker than the congruence we obtained using the Chinese remainder theorem.

This leads us to the following strengthening of Euler's theorem. If the prime factorization of n is $n = p_1^{k_1} \cdots p_r^{k_r}$, then $x^{f(n)} \equiv 1 \pmod{n}$, where

$$f(n) = \operatorname{lcm}(\varphi(p_1^{k_1}), \varphi(p_2^{k_2}), \ldots, \varphi(p_r^{k_r})).$$

Advanced comment. This $f(n)$ is almost the minimal value $\lambda(n)$ such that $x^{\lambda(n)} \equiv 1 \pmod{n}$. The only improvement that can be made is that, in the above, $\varphi(2^m)$ may be replaced with $\frac{1}{2}\varphi(2^m)$ if $m \geqslant 3$. This is known as Carmichael's theorem. □

Problem 8. Let a, b be positive integers.

(a) Suppose that $x^a \equiv 1 \pmod{n}$ and $x^b \equiv 1 \pmod{n}$. Show that $x^{\gcd(a,b)} \equiv 1 \pmod{n}$.

(b) Use the previous result to find all solutions to $x^{10} \equiv 1 \pmod{2017}$.

(c) Use the previous result to find all solutions to $x^{10} \equiv 1 \pmod{2018}$.

(d) On the other hand, there are 16 solutions to $x^{10} \equiv 1 \pmod{2016}$. Explain!

Solution.

(a) By Bezout's identity, we find integers r, s such that $ra + sb = \gcd(a, b)$. Hence,

$$x^{\gcd(a,b)} = x^{ra+sb} = (x^a)^r \cdot (x^b)^s \equiv 1^r \cdot 1^s \equiv 1 \pmod{n}.$$

(b) Note that a solution x is necessarily coprime to 2017 (why?!). By Fermat's little theorem, $x^{2016} \equiv 1 \pmod{2017}$. Since $\gcd(2016, 10) = 2$, we conclude (using the first part) that $x^2 \equiv 1 \pmod{2017}$. Since 2017 is a prime, this congruence has only the solutions $x \equiv \pm 1 \pmod{2017}$.

(c) Again, a solution x is necessarily coprime to 2018. By Euler's theorem, $x^{1008} \equiv 1 \pmod{2018}$ because $\phi(2018) = \phi(2)\phi(1009) = 1008$. Since $\gcd(1008, 10) = 2$, we conclude that $x^2 \equiv 1 \pmod{2018}$.

By the Chinese remainder theorem (CRT):

$$\begin{aligned} & x^2 \equiv 1 \pmod{2018} \\ \iff\ & x^2 \equiv 1 \pmod{2} \text{ and } x^2 \equiv 1 \pmod{1009} \\ \iff\ & x \equiv \pm 1 \pmod{2} \text{ and } x \equiv \pm 1 \pmod{1009} \\ \iff\ & x \equiv 1 \pmod{2} \text{ and } x \equiv \pm 1 \pmod{1009} \end{aligned}$$

[Recall that, modulo a prime, the congruence $x^2 \equiv 1$ has only the solutions $x \equiv \pm 1$.]

We conclude that the only solutions are $x \equiv +1 \pmod{2018}$.

[Make sure that this argument makes sense! Review Problem 3 if in doubt.]

(d) Once more, a solution x is necessarily coprime to 2016. By Euler's theorem, $x^{576} \equiv 1 \pmod{2016}$. Since $\gcd(576, 10) = 2$, we conclude, again, that $x^2 \equiv 1 \pmod{2016}$. Since $2016 = 2^5 \cdot 3^2 \cdot 7$, the CRT implies:

$$\begin{aligned} & x^2 \equiv 1 \pmod{2016} \\ \iff\ & x^2 \equiv 1 \pmod{2^5} \text{ and } x^2 \equiv 1 \pmod{3^2} \text{ and } x^2 \equiv 1 \pmod{7} \end{aligned}$$

Each of the three congruences has (at least) two solutions (namely, $x \equiv \pm 1$), so that we are going to have (at least) a total of $2 \cdot 2 \cdot 2 = 8$ solutions. That we actually have $16 = 4 \cdot 2 \cdot 2$ solutions modulo 2016 is due to the fact that $x^2 \equiv 1 \pmod{2^5}$ actually has 4 instead of just 2 solutions (namely, $x \equiv \pm 1, \pm 15 \pmod{2^5}$).

Just in case you're curious, the 16 solutions are

$$\pm 1, \pm 127, \pm 433, \pm 449, \pm 559, \pm 575, \pm 881, \pm 1007$$

modulo 2016. □

Problem 9.

(a) Among the numbers $1, 2, \ldots, 2019$, how many are coprime to 2019? (673 is a prime.)

(b) Carefully state Euler's theorem.

(c) Carefully state the Chinese remainder theorem.

(d) Carefully state Euler's criterion for quadratic residues.

(e) Use Euler's criterion for quadratic residues to determine whether 3 is a quadratic residue modulo 19.

(f) Use Euler's criterion for quadratic residues to determine whether 3 is a quadratic residue modulo 23.

(g) If the prime factorization of n is $n = p_1^{k_1} \cdots p_r^{k_r}$, what does $\phi(n)$ evaluate to?

Solution.

(a) $\phi(2019) = \phi(3)\phi(673) = 2 \cdot 672 = 1344$

(b) If $n \geqslant 1$ and $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.

(c) Let $n_1, n_2, \ldots, n_r$ be positive integers with $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then the system of congruences

$$x \equiv a_1 \pmod{n_1}, \quad \ldots, \quad x \equiv a_r \pmod{n_r}$$

has a simultaneous solution, which is unique modulo $n = n_1 \cdots n_r$.

(d) Let p be an odd prime and a an invertible residue modulo p. Then a is a quadratic residue modulo p if and only if $a^{(p-1)/2} \equiv 1$.

(e) We compute $3^9 \pmod{19}$ using binary exponentiation: $3^2 = 9$, $3^4 = 81 \equiv 5$, $3^8 \equiv 25 \equiv 6 \pmod{19}$ so that $3^9 \equiv 3 \cdot 6 \equiv -1 \pmod{19}$. Hence, by Euler's criterion, 3 is not a quadratic residue modulo 19.

(f) We compute $3^{11} \pmod{23}$ using binary exponentiation: $3^2 = 9$, $3^4 = 81 \equiv -11$, $3^8 \equiv 121 \equiv 6 \pmod{23}$ so that $3^{11} \equiv 3 \cdot 9 \cdot 6 \equiv 1 \pmod{23}$. Hence, by Euler's criterion, 3 is a quadratic residue modulo 23.

(g) If the prime factorization of n is $n = p_1^{k_1} \cdots p_r^{k_r}$, then $\phi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right)$. □

Problem 10.

(a) You wonder whether 33, 660, 239 is a prime. A (comparatively) quick computation shows that $2^{33660238} \equiv 20364778 \pmod{33660239}$. What do you conclude?

(b) You wonder whether 39, 916, 801 is a prime. A quick computation shows that $2^{39916800} \equiv 1 \pmod{39916801}$. What do you conclude?

(c) What does it mean for a to be a Fermat liar modulo n?

(d) What does it mean for n to be an absolute pseudoprime?

(e) Outline the Fermat primality test. What makes this a heuristic test?

(f) Using Fermat's little theorem and base 3, show that 341 is not a prime.

(g) Is 2 a Fermat liar modulo 341?

These computations are tedious to do by hand. Do make sure though that the idea and the procedure are clear.

Solution.

(a) This proves that 33660239 is not a prime. Because, if it was a prime, then $2^{33660238} \equiv 1 \pmod{33660239}$ by Fermat's little theorem.

[Indeed, $33660239 = 269 \cdot 125,131$ but finding that factorization is a more difficult task!]

(b) We still don't know whether 39916801 is a prime or not. There is two possibilities: either 39916801 is a prime, or 39916801 is a pseudoprime to base 2 (people also say that 2 is a "Fermat liar" in that case).

[Actually, 39916801 is a prime.]

(c) It means that $a^{n-1} \equiv 1 \pmod{n}$ despite n being composite. In other words, with respect to the base a, n behaves like a prime would by Fermat's little theorem.

(d) These are numbers n for which every residue a is either a Fermat liar modulo n or $\gcd(a, n) > 1$.

(e) Fermat primality test:

Input: number n and parameter k indicating the number of tests to run
Output: "not prime" or "possibly prime"
Algorithm:

```
Repeat $k$ times:
    Pick a random number $a$ from $\{2, 3, ..., n-2\}$.
    If $a^{n-1} \not\equiv 1 \pmod{n}$, then stop and output "not prime".
Output "possibly prime".
```

The test is heuristic because it is not designed to decide with absolute certainty whether a number is a prime. More specifically, if it claims that a number is composite, then we actually do have certainty that the number is indeed composite (but don't know its factors). However, the test is unable to prove that a number is prime; if we choose the number of iterations k large enough, then we have strong reason to believe that n is a prime (one can prove that, if we do not deal with an absolute pseudoprime [which are very rare], then there is only a probability of 2^{-k} that we mistakenly label a composite number as probably prime).

(f) $3^{340} \equiv 56 \not\equiv 1 \pmod{341}$ so that, by Fermat's little theorem, 341 cannot be a prime.

Of course, computing that $3^{340} \equiv 56 \pmod{341}$ requires some work. In the absence of knowing the prime factorization of 341, we resort to direct binary exponentiation (see comment below) and $340 = (101010100)_2 = 256 + 64 + 16 + 4$. Here are the intermediate values we get modulo 341: $3^2 \equiv 9$, $3^4 \equiv 81$, $3^8 \equiv 82$, $3^{16} \equiv 245$, $3^{32} \equiv 9$ (so that, now, the values repeat), $3^{64} \equiv 81$, $3^{128} \equiv 82$, $3^{256} \equiv 245$.

Useful observation. Note that we could have saved some work by exploiting $3^{32} \equiv 3^2 \pmod{341}$, which implies $3^{30} \equiv 1 \pmod{341}$. Since $340 \equiv 10 \pmod{30}$, we find that $3^{340} \equiv 3^{10} = 3^2 \cdot 3^8 \equiv 56 \pmod{341}$.

(g) We need to compute $2^{340} \pmod{341}$. We proceed using binary exponentiation as in the previous part. The values we get modulo 341 are: $2^2 = 4$, $2^4 = 16$, $2^8 = 256$, $2^{16} = 64$, $2^{32} = 4$, so that, again, values repeat.

In the end, we find that $2^{340} \equiv 1 \pmod{341}$. This means that 2 is indeed a Fermat liar modulo 341 (because we already know that 341 is not an actual prime).

Useful observation. Again, we can save a lot of work by exploiting $2^{32} \equiv 2^2 \pmod{341}$, which implies $2^{30} \equiv 1 \pmod{341}$. As before, we conclude that $2^{340} \equiv 2^{10} = 2^2 \cdot 2^8 \equiv 1 \pmod{341}$.

Comment. If we know the factorization of 341 then we can cut down on our work a little bit by using the Chinese remainder theorem and Euler's theorem (but realize that if we have to ask questions like whether 341 is a prime, then we wouldn't know this factorization and wouldn't be able to apply these theorems). □

Problem 11.

(a) State Wilson's theorem.

(b) List all quadratic residues modulo 21.

(c) What is the number of invertible quadratic residues modulo 91? Modulo 101? Modulo 165?

Solution.

(a) If p is a prime, then $(p-1)! \equiv -1 \pmod{p}$.

(b) $0^2 = 0$, $(\pm 1)^2 = 1$, $(\pm 2)^2 = 4$, $(\pm 3)^2 = 9$, $(\pm 4)^2 = 16$, $(\pm 5)^2 \equiv 4$, $(\pm 6)^2 \equiv 15$, $(\pm 7)^2 \equiv 7$, $(\pm 8)^2 \equiv 1$, $(\pm 9)^2 \equiv 18$, $(\pm 10)^2 \equiv 16$

In summary, the quadratic residues are $0, 1, 4, 7, 9, 15, 16, 18$.

(The invertible quadratic residues are $1, 4, 16$. That's $\phi(21)/4 = \frac{\phi(3)\phi(7)}{4} = 3$ many.)

(c) Since $91 = 7 \cdot 13$ is a product of two distinct odd primes, there are $\frac{1}{4}\phi(91) = \frac{6 \cdot 12}{4} = 18$ invertible quadratic residues modulo 91.

Since 101 is a prime, there are $\frac{\phi(101)}{2} = 50$ invertible quadratic residues modulo 101.

Since $165 = 3 \cdot 5 \cdot 11$ is a product of three distinct odd primes, there are $\frac{1}{8}\phi(165) = \frac{2 \cdot 4 \cdot 10}{8} = 10$ invertible quadratic residues modulo 165. □