Midterm #3: practice

MATH 311 — Intro to Number Theory
midterm: Thursday, Nov 17

Please print your name:

Calculators will not be permitted on the exam. The numbers on the exam will be suitable for calculating by hand.

Problem 1. 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 2. 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 3. 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.

(c) Compare the two results!

Bonus: Can you come up with a strengthening of Euler's theorem?

Solution.

(a) Since $\phi(323) = 323\left(1 - \frac{1}{17}\right)\left(1 - \frac{1}{19}\right) = 288$, 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 $x^{144} \equiv (x^{18})^8 \equiv 1 \pmod{19}$.

(c) 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 4. 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) On the other hand, there are 16 solutions to $x^{10} \equiv 1 \pmod{2016}$. What is different in this case?

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 that $x^2 \equiv 1 \pmod{2017}$. Since 2017 is a prime, this congruence has only the solutions $x \equiv \pm 1 \pmod{2017}$. (We established this in Problem 2 of Homework 4. Make sure that you recall the argument and why it is crucial that 2017 is a prime.)

(c) Again, 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 that $x^2 \equiv 1 \pmod{2016}$. However, 2016 is not a prime and so this congruence actually has more solutions than just $x \equiv \pm 1 \pmod{2016}$.

Comment. In fact, it has the 16 solutions

$$1, 127, 433, 449, 559, 575, 881, 1007, 1009, 1135, 1441, 1457, 1567, 1583, 1889, 2015$$

modulo 2016. Clearly, each of these also solves $x^{10} \equiv 1 \pmod{2016}$. Problem 9 below makes it transparent where these "extra" solutions are coming from. In short, by the Chinese remainder theorem, the congruence modulo $2016 = 2^5 \cdot 3^2 \cdot 7$ breaks into congruences modulo 2^5, 3^2 and 7; in each of these three cases, we get at least the two solutions ± 1, which we can combine in $2 \cdot 2 \cdot 2 = 8$ different ways to get 8 solutions modulo 2016. 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, $x \equiv \pm 1, \pm 15 \pmod{2^5}$)). □

Problem 5.

(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?

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.] □

Problem 6.

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

(b) Is 341 a pseudoprime to the base 2?

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

Solution.

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

Of course, computing that $3^{340} \equiv 56$ (mod 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 $3^{340} \equiv 3^{10} = 3^2 \cdot 3^8 \equiv 56 \pmod{341}$.

(b) We need to compute 2^{340} (mod 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 341 is a pseudoprime to the base 2 (because we already know that 341 is not an actual prime).

Useful observation. Again, we can save a lot of work by exploiting $2^{32} \equiv 2^2$ (mod 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 7.

(a) Among the numbers $1, 2, \ldots, 2016$, how many are coprime to 2016?

(b) Carefully state Euler's theorem.

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

(d) Carefully state Wilson's theorem.

Solution.

(a) This just asks for $\phi(2016)$.

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

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

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

Problem 8.

(a) What does it mean for n to be a pseudoprime to base a?

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

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

Solution.

(a) It means that n is composite but satisfies $a^n \equiv a \pmod{n}$. In other words, it behaves like a prime would by Fermat's little theorem.

Sometimes the condition $a^n \equiv a \pmod{n}$ is replaced with $a^{n-1} \equiv 1 \pmod{n}$. That makes no difference unless $\gcd(a, n) \neq 1$ (in which case we learned about a divisor of n).

(b) These are numbers which are pseudoprime to any base $a > 1$.

(c) 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). But 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 (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). □

Problem 9.

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

(b) Can you predict how many solutions the congruence $x^2 \equiv 1 \pmod{210}$ is going to have?

Solution.

(a) Note that $105 = 3 \cdot 5 \cdot 7$. By the Chinese remainder theorem, 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 $x \equiv \pm 1$. (Again, we established this in Problem 2 of Homework 4.) Using the Chinese remainder theorem, these combine in $2 \cdot 2 \cdot 2 = 8$ different ways to a solution modulo 105. For instance, one the 8 possibilities is

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

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.

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.

(b) 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.

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

Problem 10.

(a) Which number is represented by the continued fraction $[1; 2, 1, 2, 1, 2]$?

(b) Determine all convergents of $[1; 2, 1, 2, 1, 2]$.

(c) Which number is represented by the infinite continued fraction $[1; 2, 1, 2, 1, 2, 1, 2, \ldots]$?

(d) Compare, numerically, the first six convergents (computed above) to the value of the infinite continued fraction.

Solution.

(a) $[1; 2, 1, 2, 1, 2] = 1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{2}}}}} = \frac{41}{30}$

Comment. Of course, we can simplify this continued fraction directly. But that is a bit time consuming and prone to errors. A better is way is to compute the convergents recursively as we do in the next part.

(b) The convergents are $C_0 = 1$, $C_1 = [1; 2] = 1 + \frac{1}{2} = \frac{3}{2}$, $C_2 = [1; 2, 1] = 1 + \frac{1}{2 + \frac{1}{1}} = \frac{4}{3}$.

We can continue like that but the computations will get more involved. Instead, we should proceed recursively. Recall from class that the convergents $C_n = \frac{p_n}{q_n}$ of $[a_0; a_1, a_2, \ldots]$ are characterized by

$$\begin{array}{lcl} p_k = a_k p_{k-1} + p_{k-2} & & q_k = a_k q_{k-1} + q_{k-2} \\ \text{with } p_{-2} = 0, \quad p_{-1} = 1 & \text{and} & \text{with } q_{-2} = 1, \quad q_{-1} = 0 \end{array}.$$

The corresponding calculations of p_n and q_n are as follows:

n	-2	-1	0	1	2	3	4	5
a_n			1	2	1	2	1	2
p_n	0	1	1	3	4	11	15	41
q_n	1	0	1	2	3	8	11	30
C_n			1	$\frac{3}{2}$	$\frac{4}{3}$	$\frac{11}{8}$	$\frac{15}{11}$	$\frac{41}{30}$

(c) Write $x = [1; 2, 1, 2, 1, 2, 1, 2, \ldots]$. Then, $x = 1 + \frac{1}{2 + \frac{1}{1 + \frac{1}{2 + \frac{1}{1 + \ldots}}}} = 1 + \frac{1}{2 + \frac{1}{x}}$.

The equation $x = 1 + \frac{1}{2 + \frac{1}{x}}$ simplifies to $x - 1 = \frac{x}{2x + 1}$. Further (note that, clearly $x \neq -\frac{1}{2}$ so that $2x + 1 \neq 0$) simplifies to $(x - 1)(2x + 1) = x$ or $2x^2 - 2x - 1 = 0$, which has the solutions $x = \frac{2 \pm \sqrt{4 + 8}}{4} = \frac{1 \pm \sqrt{3}}{2}$.

Since $\frac{1 + \sqrt{3}}{2} \approx 1.366$ and $\frac{1 - \sqrt{3}}{2} \approx -0.366$, we conclude that $[1; 2, 1, 2, 1, 2, 1, 2, \ldots] = \frac{1 + \sqrt{3}}{2}$.

(d) $C_0 = 1$, $C_1 = \frac{3}{2} = 1.5$, $C_2 = \frac{4}{3} \approx 1.333$, $C_3 = \frac{11}{8} = 1.375$, $C_4 = \frac{15}{11} \approx 1.364$, $C_5 = \frac{41}{30} \approx 1.367$

These values quickly approach $\frac{1+\sqrt{3}}{2} \approx 1.366$ in the expected alternating fashion. □

Problem 11.

(a) Express the numbers $\frac{252}{193}$ and $-\frac{337}{221}$ as a simple continued fraction.

(b) Is this the unique simple continued fraction representing $\frac{252}{193}$? Explain!

Solution.

(a) The simplest way to obtain the continued fraction for $\frac{252}{193}$ is via the Euclidian algorithm:

$$252 = \boxed{1} \cdot 193 + 59, \quad 193 = \boxed{3} \cdot 59 + 16, \quad 59 = \boxed{3} \cdot 16 + 11, \quad 16 = \boxed{1} \cdot 11 + 5, \quad 11 = \boxed{2} \cdot 5 + 1, \quad 5 = \boxed{5} \cdot 1 + 0$$

Hence, $\frac{252}{193} = [1; 3, 3, 1, 2, 5]$.

To determine a simple continued fraction for $-\frac{337}{221}$, we first write $-\frac{337}{221} = -2 + \frac{105}{221} = \boxed{-2} + \frac{1}{\frac{221}{105}}$. We then proceed using the Euclidian algorithm applied to $\frac{221}{105}$.

$$221 = \boxed{2} \cdot 105 + 11, \quad 105 = \boxed{9} \cdot 11 + 6, \quad 11 = \boxed{1} \cdot 6 + 5, \quad 6 = \boxed{1} \cdot 5 + 1, \quad 5 = \boxed{5} \cdot 1 + 0.$$

Combined, $-\frac{337}{221} = [-2; 2, 9, 1, 1, 5]$.

(b) No, a finite continued fraction can always be expressed in two ways because of the simple relation $[a_0; a_1, a_2, \ldots, a_n] = [a_0; a_1, a_2, \ldots, a_n - 1, 1]$, assuming $a_n > 1$. In this case, we also have $\frac{252}{193} = [1; 3, 3, 1, 2, 4, 1]$. □

— It is also a very good idea to review the problems from Homework 5 as well as the previous practice problems. —