Midterm Exam

Math 110
10 February 2015
Jenny Wilson

Name: ______________________________

Instructions: This exam has 10 questions for a total of 40 points plus 5 bonus points.

You may bring in a basic calculator. No books, notes, cell phones, or advanced calculators are permitted. Scratch paper is available.

Please show your work clearly in the space provided. Solutions may not receive full credit without legible work shown. Partial credit may be given for correct work, even if there is a mistake in the final answer.

You have 75 minutes to complete the exam. If you finish early, consider checking your work for accuracy.

Jenny is available to answer questions around the corner from the classroom.

Question	Points	Score
1	3	
2	5	
3	4	
4	2	
5	2	
6	5	
7	4	
8	10	
9	5	
10	0	
Total:	40	

1. (3 points) Compute the set of all integer solutions (u, v) to the equation

$$102u + 45v = 3.$$

You do not need to formally prove that your answer is correct, but please show your work.

We first find a particular integer solution (u, v) using the Euclidean algorithm.

$$\begin{aligned} 102 &= 2(45) + 12 \\ 45 &= 3(12) + 9 \\ 9 &= 1(12) + 3 \\ 12 &= 4(3) \end{aligned}$$

$$\begin{aligned} 3 &= 12 - 9 \\ 3 &= 12 - (45 - 3(12)) \\ 3 &= 4(12) - (45) \\ 3 &= 4(102 - 2(45)) - (45) \\ 3 &= 4(102) - 9(45) \end{aligned}$$

We have found a particular solution $u = 4, v = -9$. From Homework 1, we know that the set of all solutions is:

$$\left\{ \left(u + \frac{45}{3}t, v - \frac{102}{3}t \right) \mid t \in \mathbb{Z} \right\} = \{(4 + 15t, -9 - 34t) \mid t \in \mathbb{Z}\}$$

Remarks on grading: Students received 2/3 for finding a particular solution, and 3/3 for correctly writing the set of all solutions.

Students earned 2.5/3 for identifying most solutions (eg, $(4 + 45t, -9 - 102t)$ for $t \in \mathbb{Z}$), or for a solution with 15 and 34 reversed.

2. (5 points) Alonso and Benita are communicating using RSA. Benita publishes the modulus $n = 3131$ and the encryption exponent $e = 353$. Alonso returns the encrypted message 686. Given the factorization $n = (31)(101)$, decrypt Alonso's message. Show your work.

You may find the following helpful:

$686^2 \equiv 946 \pmod{3131}$
$946^2 \equiv 2581 \pmod{3131}$
$2581^2 \equiv 1924 \pmod{3131}$
$1924^2 \equiv 934 \pmod{3131}$
$934^2 \equiv 1938 \pmod{3131}$
$1938^2 \equiv 1775 \pmod{3131}$
$1775^2 \equiv 839 \pmod{3131}$
$839^2 \equiv 2577 \pmod{3131}$

Our first step is to find the decryption exponent, d, which should be the multiplicative inverse to e modulo $\phi(n)$. We have:

$$\phi(3131) = \phi(31)\phi(101) = (30)(100) = 3000.$$

We use the Euclidean algorithm to find the multiplicative inverse for $e \equiv 353 \pmod{3000}$.

$$\begin{aligned} 3000 &= 8(353) + 176 \\ 353 &= 2(176) + 1 \end{aligned}$$

$$\begin{aligned} 1 &= 353 - 2(176) \\ 1 &= 353 - 2(3000 - 8(353)) \\ 1 &= 17(353) - 2(3000) \end{aligned}$$

We find that $d = 17$ is a multiplicative inverse to $e \equiv 353 \pmod{3000}$.

To compute the plaintext m, we need to compute $686^d \equiv 686^{17} \pmod{3131}$.

$$\begin{aligned} 686^{17} &\equiv (686^{16})(686) \pmod{3131} \\ &\equiv (686^{2^4})(686) \pmod{3131} \\ &\equiv (934)(686) \pmod{3131} \quad \text{from the list of powers above} \\ &\equiv 640724 \pmod{3131} \\ &\equiv 2000 \pmod{3131} \end{aligned}$$

We conclude that Alonso's message is $2000 \pmod{3131}$.

Remarks on grading: The rough grade breakdown is 1 point for properly computing $\phi(n)$, 2 points for successfully computing the decryption exponent 17, and 2 points for successfully computing 686^{17}.

Some students made errors seemingly because they miscopied a number from one point in the computation to another. These are minor and non-mathematical errors and so were not penalized if the method was otherwise correct.

In situations where students could reasonably double-check the end result of their computation (such as verifying $17(353)-2(3000)=1$) then arithmetic errors were penalized by -0.5 points. In instances where it is difficult to double-check the correctness of the solution, minor arithmetic mistakes were not penalized if the method was otherwise correct.

Students lost 2 points for computing the inverse of e modulo n instead of modulo $\phi(n)$.

3. (4 points) Akira wishes to send a message to Bo using the ElGamal public key cryptosystem. Describe the steps in their exchange, and briefly explain why it is hard for the eavesdropper Evita to intercept their message.

Akira and Bo perform the following steps:

- Bo chooses a large prime p, a primitive root α of p, and a secret random exponent $a \in \mathbb{Z}$, with $1 < a < (p-2)$.
- Bo publishes p, $\alpha \pmod{p}$ and $\alpha^a \pmod{p}$.
- Akira breaks the message into blocks m with $0 \leq m < p$.
- For each block m, Akira chooses a secret exponent $k \in \mathbb{Z}$, with $1 < k < (p-2)$.
- Akira publishes $\alpha^k \pmod{p}$ and $(\alpha^a)^k m \pmod{p}$.
- Bo decrypts $m \equiv (\alpha^k)^{-a}(\alpha^{ak}m) \pmod{p}$.

Evita has access to the congruence classes $\alpha, \alpha^a, \alpha^k$, and $\alpha^{ak}m$ modulo p. However, it is believed to be computationally very difficult to compute a, k, or α^{ak} from this data, and so Evita cannot easily decrypt the message.

Approximate grade breakdown: 3 points for correctly describing the exchange; 1 point for stating that the security of the system is based on the difficulty of the discrete log problem.

The description of the exchange must include an explanation of all the variables involved: the letters $p, \alpha, a, \beta, k, m, t, r$ do not mean anything until they are defined. Descriptions of fragments of Bo and Akira's exchange including undefined variables earned up to 0.5 out of 3 points.

Some examples of common errors are listed below. Students lost 0.5 points for errors or 0.5 points for two minor errors.

- (Minor error) The question states that Akira wishes to send a message to Bo, though several students outlined steps for Bo to send a message to Akira.
- (Minor error) Bo (or Akira) must select the large prime p before the congruence class α, since α must be defined in terms of p; it is a primitive root of p. Several students listed the quantities selected in the wrong order.
- (Minor error) If Akira's message is too long, it should be broken into smaller numbers m of size less than p. Akira should choose a different value of k for each message m. Several students listed the steps "break m into pieces" and "choose integer k" in the wrong order.
- The exponents a and k should be either integers or (by Fermat's Little Theorem) congruence classes modulo $(p-1)$. They should not be congruence classes modulo

p, since exponentiating elements of $\mathbb{Z}/p\mathbb{Z}$ by an exponent $[d]$ in $\mathbb{Z}/p\mathbb{Z}$ is not a well-defined operation; it would yield different numbers for different representatives of the class $[d]$.

- Evita cannot easily compute α^{ak} given the publicly available information. This is fortunate, since this would enable her to compute $m \equiv (\alpha^{ak})^{-1}(\alpha^{ak}m) \pmod{p}$.

4. (2 points) Suppose that x is an integer satisfying $19^x \equiv 2 \pmod{29}$. Given that 19 is a primitive root of 29, is x even or odd?

   No formal justification needed, but please show your work.

   If α is a primitive root modulo a prime p, then a solution x to $\alpha^x \equiv b \pmod{p}$ will be even if $b^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ and odd if $b^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. We compute:

$$\begin{aligned}
2^{\frac{29-1}{2}} &\equiv 2^{14} &\pmod{29}\\
&\equiv 2^8 2^4 2^2 &\pmod{29}\\
&\equiv (256)(16)(4) &\pmod{29}\\
&\equiv (24)(16)(4) &\pmod{29}\\
&\equiv 1536 &\pmod{29}\\
&\equiv 28 &\pmod{29}\\
&\equiv -1 &\pmod{29}
\end{aligned}$$

   We conclude that x must be odd.

   Approximate grading breakdown: Students earn 1.5 points for identifying what computation should be done, and 0.5 points for correctly exponentiating.

   An answer of ”even” or ”odd” received no credit without supporting calculations shown.

   Students could also receive full credit for correctly solving the problem by other methods (such as solving for x by a brute force) but should note that this approach would be infeasible if the numbers were much larger.

5. (2 points) Ahmad and Brianna wish to use the Diffie–Hellman key exchange to establish a secret shared key K. Ahmad publishes the prime $p = 1009$ and the primitive root 51 (mod 1009). Brianna selects the exponent $y = 3$ and publishes $51^3 \equiv 472 \pmod{1009}$. Ahmad selects an exponent x publishes $51^x \equiv 22 \pmod{1009}$. What key K do they establish?

   No formal justification needed, but please show your work.

   The key $K \equiv 51^{3x} \pmod{1009} \equiv 22^3 \pmod{1009}$.

   We compute $22^3 = 10648 \equiv 558 \pmod{1009}$.

   Approximate grading breakdown: Students earn 1.5 points for identifying what computation should be done, and 0.5 points for correctly exponentiating.

   Students received up to 0.5 points credit for a statement such as $K = \alpha^{xy}$ or $K = 51^{3x}$ but no additional credit if they did not know how to proceed from there, or erroneously asserted that $\alpha^{xy} = \alpha^x \alpha^y$.

6. (5 points) Given the factorization $989 = (23)(43)$, find all solutions to the equation

$$x^2 \equiv 6 \pmod{989}.$$

Show your work.

According to the Chinese Remainder Theorem, the set of solutions x can be identified with all combinations of solutions

$$x^2 \equiv 6 \pmod{23} \qquad \text{and} \qquad x^2 \equiv 6 \pmod{43}.$$

Since 23 and 43 are both primes p congruent to 3 modulo 4, we know that $\pm 6^{\frac{p+1}{4}}$ will give us all square roots of 6 modulo p, if any exist at all.

Alternatively, we can find square roots of 6 modulo p by squaring positive integers up to $p - 1$ and reducing mod p to see if we find 6. Or, perhaps the easiest method with a simple calculator: adding multiples of p to 6 until we find an integer that we recognize as a square, in this case, $6 + 5(23) = 121 = 11^2$, and $6 + 43 = 49 = 7^2$.

By the first method, we find:

$$\begin{aligned} 6^2 = 36 &\equiv 13 \pmod{23} \\ 6^4 \equiv 13^2 &\equiv 8 \pmod{23} \end{aligned}$$

$$\begin{aligned} 6^{\frac{23+1}{4}} &\equiv 6^6 \pmod{23} \\ &\equiv 6^4 6^2 \pmod{23} \\ &\equiv (8)(13) \pmod{23} \\ &\equiv 104 \pmod{23} \\ &\equiv 12 \pmod{23} \end{aligned}$$

$$\begin{aligned} 6^2 = 36 &\equiv 7 \pmod{43} \\ 6^4 \equiv 7^2 &\equiv 6 \pmod{43} \\ 6^8 \equiv 6^2 &\equiv 7 \pmod{23} \end{aligned}$$

$$\begin{aligned} 6^{\frac{43+1}{4}} &\equiv 6^{11} \pmod{43} \\ &\equiv 6^8 6^2 6 \pmod{43} \\ &\equiv (7)(7)(6) \pmod{43} \\ &\equiv 194 \pmod{43} \\ &\equiv 36 \pmod{43} \end{aligned}$$

We can check in both cases that these numbers do square to 6 modulo 23 and 43, and so our solutions will be all solutions:

$$x \equiv 11 \text{ or } 12 \pmod{23} \qquad \text{and} \qquad x \equiv 7 \text{ or } 36 \pmod{43}.$$

To find the solutions, we use the Chinese Remainder Theorem to integers (u, v) such that $43u + 23v = 1$.

$$\begin{aligned}
43 &= 23 + 20\\
23 &= 20 + 3\\
20 &= 6(3) + 2\\
3 &= 2 + 1
\end{aligned}$$

$$\begin{aligned}
1 &= 3 - 2\\
1 &= 3 - (20 - 6(3))\\
1 &= 7(3) - (20)\\
1 &= 7(23 - 20) - (20)\\
1 &= 7(23) - 8(20)\\
1 &= 7(23) - 8(43 - 23)\\
1 &= 15(23) - 8(43)
\end{aligned}$$

Thus our four solutions x modulo 989 are the following:

$$\begin{aligned}
x &\equiv 15(23)(7) - 8(43)(11) \equiv -1369 \equiv 609 \pmod{989}\\
x &\equiv 15(23)(7) - 8(43)(12) \equiv -1713 \equiv 265 \pmod{989}\\
x &\equiv 15(23)(36) - 8(43)(11) \equiv 8636 \equiv 724 \pmod{989}\\
x &\equiv 15(23)(36) - 8(43)(12) \equiv -1713 \equiv 380 \pmod{989}
\end{aligned}$$

The approximate grading breakdown: 1.5 points for knowing the correct outline of the proof (reducing modulo 23 and 43, finding roots of 6, and using the Chinese Remainder Theorem to recombine these solutions), 1.5 points for correctly finding square roots of 6 modulo 23 and 43, 1 point for correctly finding integer solutions u, v to $43u + 23v = 1$, and 1 point for correctly computing the four values of x modulo 989.

If students computed square roots of 6 modulo $p = 23, 43$ by computing $6^{\frac{p+1}{4}} \pmod{p}$, then they lost 0.5 points if they neglected to check that these classes are square roots of $6 \pmod{p}$, and not square roots of $-6 \pmod{p}$.

Students lost marks if they made significant jumps in the computation without showing any explicit work, even if their final solution was correctly.

7. (4 points) (a) Given that $\gcd(8647, 111) = 1$, compute the Jacobi symbol $\left(\frac{111}{8647}\right)$. Show your work.

$$\begin{aligned}
\left(\frac{111}{8647}\right) &= -\left(\frac{8647}{111}\right) && \text{since } 111 \equiv 8647 \equiv 3 \pmod 4 \\
&= -\left(\frac{100}{111}\right) && \text{since } 8647 \equiv 100 \pmod{111} \\
&= -\left(\frac{10}{111}\right)^2 \\
&= -1 && \text{since } 1^2 = (-1)^2 = 1.
\end{aligned}$$

Part (a) is worth 2 points.

Students lose 1 point for misapplying the law of quadratic reciprocity, and 0.5 points for other errors.

Students receive full points for this question for correct steps leading to a correct answer, even if found using an inefficient method.

(b) What can you conclude (if anything) about whether the congruence 111 is a square modulo 8647? Justify your answer.

We can conclude that 111 is **not** a square modulo 8647.

Suppose that 8647 had prime factorization $8647 = p_1^{d_1} p_2^{d_2} \cdot p_r^{d_r}$ for some set of primes $p_1, p_2, \ldots p_r$. Then by definition the Jacobi symbol is the product of Legendre symbols:

$$\left(\frac{111}{8647}\right) := \left(\frac{111}{p_1}\right)^{d_1} \left(\frac{111}{p_2}\right)^{d_2} \cdots \left(\frac{111}{p_r}\right)^{d_r}.$$

Because $\left(\frac{111}{8647}\right) = -1$ by part (a), we know that at least one of the factors $\left(\frac{111}{p_i}\right) = -1$, and so 111 is not a square modulo some prime divisor p_i of 8647. If there were some integer x such that $x^2 \equiv 111 \pmod{8647}$, then reducing modulo p_i we would find that $x^2 \equiv 111 \pmod{p_i}$, a contradiction. So there must be no such square root x of 111 modulo 8647.

Part (b) is out of 2 points. The solution to part (b) depends on whether the student computed that the symbol is -1 or 1 in part (a).

In general, a student receives 0.5 points for a statement of the correct answer. (If the symbol was -1, then 111 is definitely not a square modulo 8647, if the symbol was 1 then 111 may or may not be a square modulo 8647.)

Roughly speaking, a student received an additional 0.5 points for stating the definition of the Jacobi symbol (or otherwise relating $\left(\frac{111}{8647}\right)$ to the Legendre symbols $\left(\frac{111}{p_i}\right)$ for prime factors p_i of 8647.) Students received 0.5 points for pointing out the connection between the Legendre symbol and the existence of square roots of 111 modulo p_i. Students received the last 0.5 points for stating the relationship between whether 111 is square modulo 8647 and whether 111 is a square modulo the prime factors of 8647.

8. (10 points) State whether each of the following assertions is always true by writing "True" or "False". No justification necessary.

(a) The congruence class [21] modulo 33 is a zero divisor.

True. Since $\gcd(21, 33) = 3 \neq 1$, we can find a nonzero congruence class (specifically, $\frac{33}{3} = 11$ and its multiples) whose product with 21 is zero modulo 33.

(b) Let $a, b, d \in \mathbb{Z}$. If $\gcd(a, b) = d$, then $\gcd\left(\frac{a}{d}, b\right) = 1$.

False. For example, $\gcd(8, 2) = 2$, and $\gcd\left(\frac{8}{2}, 2\right) = \gcd(4, 2) = 2$.

(c) The equation $15x \equiv 5 \pmod{18}$ has one or more solutions $x \in \mathbb{Z}$.

False. Since $\gcd(15, 18) = 3$ does not divide 5, there are no solutions. Otherwise, if x were a solution, reducing the equation modulo 3 would give the impossible relationship $0x \equiv 2 \pmod{3}$.

(d) If $d, n > 1$ are integers and d divides n, then each congruence class modulo d is the union of $\frac{n}{d}$ congruence classes modulo n.

True. You proved this on Homework 2.

(e) There are $(12)(26) = 312$ distinct invertible affine ciphers $f(x) = \alpha x + \beta$, for $\alpha, \beta \in \mathbb{Z}/26\mathbb{Z}$.

True. To produce an invertible affine cipher, we need to choose a unit α and any congruence class β modulo 26. Each distinct pair (α, β) gives a distinct affine function (since, for example, each function takes a different pair of values on the arguments $x = 0$ and $x = 1$). So there is an invertible affine cipher for each of the $\phi(26) = (2-1)(13-1) = 12$ units modulo 26 and each of the 26 classes modulo 26.

(f) The congruence class $[-1]$ can never be a square modulo a prime p.

False. It is true (as we proved in class) that -1 can never be a square modulo a prime p congruent to $3 \pmod{4}$, but in general it is possible for -1 to be congruent to a square modulo a prime p.
For example, $1^2 \equiv 1 \equiv -1 \pmod{2}$ and $2^2 \equiv 4 \equiv -1 \pmod{5}$, etc.

(g) Since $3^{1048} \equiv 1 \pmod{1049}$, we can conclude that 1049 is prime.

False. Although this result would be consistent with Fermat's Little Theorem in the case that 1049 were prime, it is not conclusive, as the same relationship occasionally holds modulo composite numbers n.

(h) Let p be a positive prime. Then any nonzero congruence class modulo p has either zero or two square roots.

True. We proved in class that if a congruence class has a square root b modulo a prime number p, then the set of its square roots is $\{b, -b\}$. If the congruence class is nonzero (and therefore b is nonzero), this set has two elements.

(i) If $n = pq$ is the product of two primes congruent to 3 (mod 4), and y is a unit and a square modulo n, then finding four distinct solutions to $x^2 \equiv y \pmod{n}$ is computationally equivalent to factoring n.

True. You proved this statement on Homework 4.

(j) A prime number p is a square modulo 41 if and only if 41 is a square modulo p.

True. Since $41 \equiv 1 \pmod{4}$, for every odd prime p the law of quadratic reciprocity states that $\left(\dfrac{p}{41}\right) = \left(\dfrac{41}{p}\right)$, so p is a square modulo 41 if and only if 41 is a square modulo p.

For $p = 2$, we know that $41 \equiv 1^2 \pmod{2}$ is a square, and furthermore that $\left(\dfrac{2}{41}\right) = 1$, so in this case too the statement is true.

Grading policy: 1 point for every correct true/false response, 0 points for incorrect responses. Ambiguous responses do not receive credit, for example, if both words "true" and "false" appear. Since the question states "no justification necessary", no partial credit is available for work shown.

9. (5 points) (a) Suppose $n > 0 \in \mathbb{Z}$ and a is a congruence class modulo n. Define the multiplicative order $\operatorname{ord}_n(a)$ of a.

The multiplicative order of a is defined whenever a is a unit modulo n. In this case, the order $\operatorname{ord}_n(a)$ of a is the smallest (strictly) positive integer k such that $a^k \equiv 1 \pmod{n}$.

Let $a, s, t, n \in \mathbb{Z}$. Prove that

$$a^s \equiv a^t \pmod{n} \qquad \text{if and only if} \qquad s \equiv t \pmod{\operatorname{ord}_n(a)}.$$

Let a be a unit modulo n, so that $\operatorname{ord}_n(a)$ is defined. Let $d = \operatorname{ord}_n(a)$. To prove this equivalence, we have to prove two implications:

$$\begin{aligned} s \equiv t \pmod{d} &\implies a^s \equiv a^t \pmod{n} \qquad\qquad \text{and} \\ a^s \equiv a^t \pmod{n} &\implies s \equiv t \pmod{d} \end{aligned}$$

To prove the first, suppose that $s \equiv t \pmod{d}$. This means that $s = t + d\ell$ for some $\ell \in \mathbb{Z}$. Hence,

$$a^s \equiv a^{t+d\ell} \equiv a^t (a^d)^\ell \equiv a^t (1)^\ell \equiv a^t \pmod{n}, \qquad \text{as desired.}$$

To prove the second implication, suppose that $a^s \equiv a^t \pmod{n}$. We can write $t - s = qd + r$ for some quotient $q \in \mathbb{Z}$ and remainder $r \in \mathbb{Z}$ with $0 \le r < d$. Because a is a unit modulo n, a and its powers are invertible. Multiplying both sides of the equation $a^s \equiv a^t \pmod{n}$ by the inverse of a^s, we find:

$$\begin{aligned} 1 &\equiv a^{t-s} \pmod{n} \\ &\equiv a^{qd+r} \pmod{n} \\ &\equiv (a^d)^q a^r \pmod{n} \\ &\equiv 1^q a^r \pmod{n} \\ &\equiv a^r \pmod{n} \end{aligned}$$

so $a^r \equiv 1 \pmod{n}$. But, by definition, d is the smallest positive integer k such that $a^k \equiv 1 \pmod{n}$, so the only possibility for the remainder r is $r = 0$. We conclude that $t - s = qd$, and $t \equiv s \pmod{d}$ as claimed.

Rough grade break down: 1 point for part (a), 2 points for each direction of the proof. Students commonly lost points or half-points for false statements, unjustified statements, undefined variables and other formal errors, or large amounts of content that is irrelevant to the proof.

10. (5 points (bonus)) Let $m, n, d, a, b \in \mathbb{Z}$ and suppose that $\gcd(m, n) = d$. Prove that if $a \equiv b \pmod{d}$, then there exist solutions to the simultaneous system of equations

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n}. \end{aligned}$$

There are several ways to prove this result; here is a proof that is succinct, though maybe more difficult to think up. Can you find other proofs?

Proof: Since $\gcd(m, n) = d$, we know from a result on a quiz that $\gcd\left(\frac{m}{d}, \frac{n}{d}\right) = 1$. Therefore there exist integers u, v so that

$$u\frac{m}{d} + v\frac{n}{d} = 1.$$

Multiplying this equation through by $(b - a)$, we find:

$$(b - a) = (b - a)u\frac{m}{d} + (b - a)v\frac{n}{d}$$

Rearranging, we find

$$\begin{aligned} b - (b - a)v\frac{n}{d} &= a + (b - a)u\frac{m}{d} \\ b - \frac{(b - a)vn}{d} &= a + \frac{(b - a)um}{d}. \end{aligned}$$

Because $a \equiv b \pmod{d}$ by assumption, the quantity $\frac{(b-a)}{d}$ is an integer. Thus if we define

$$x := b - \frac{(b - a)}{d}vn = a + \frac{(b - a)}{d}um$$

then x is an integer which, by construction, reduces to b modulo n and a modulo m.

Grading comments: This question is challenging, and (being a bonus question) had very little partial credit available. Students who wrote down related facts (such as "reducing modulo m to modulo d is well-defined", or a comparison to the Chinese Remainder Theorem) did not receive more than 0.5/5 points if it was unclear how these facts could be used in a proof. Students would not receive more than 1/5 unless they had made appreciable progress toward a correct proof.