

Midterm Exam 2: Thu Nov 7, in Recitation class 5:00–6:20pm, Wells A-201.

Topics

1. Methods of proof (can be combined)
 - (a) Direct proof
 - (b) Proof by cases
 - (c) Proof of the contrapositive
 - (d) Proof by contradiction
 - (e) Proof by induction (also complete induction)
2. Axioms of a Group $(G, *)$ (All variables below mean elements of G .)
 - (a) Closure: $a * b \in G$.
 - (b) Associativity: $(a * b) * c = a * (b * c)$
 - (c) Identity: There is e with $e * a = a$ and $a * e = a$ for all a .
 - (d) Inverses: For each a , there is some b with $a * b = e$ and $b * a = e$.

Extra axioms

- (e) Commutativity: $a * b = b * a$.
 - (f) Distributivity of multiplication over addition: $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$.
3. Divisibility of integers (All variables below mean integers.)
 - (a) Divisibility: $a|b$ means $b = ac$ for some c
 - (b) Properties of divisibility:
 - $a|b, c \implies a|mb+nc$ for all m, n
 - $a|b$ and $b|c \implies a|c$.
 - $a|b$ and $b|a \implies a = \pm b$.
 - (c) Prime and composite
 - Test: a is composite $\implies a$ has prime factor $p \leq \sqrt{a}$.
 - (d) Greatest common divisor $\gcd(a, b)$; relatively prime means $\gcd(a, b) = 1$.
 - (e) Division Lemma: $a = qb + r$ with $0 \leq r < b$.
 - (f) Euclidean Algorithm computes $a > b > r_1 > \dots > r_k > 0$.
 - Computes $\gcd(a, b) = r_k$.
 - Finds m, n with $\gcd(a, b) = ma + nb$.
 - Shows $e|a, b \implies e|\gcd(a, b)$
 - (g) Consequences of $\gcd(a, b) = ma + nb$
 - If $e|a$ and $e|b$, then $e|\gcd(a, b)$.
 - Euclid's Lemma: If $a|bc$ and $\gcd(a, c) = 1$, then $a|b$.
 - Prime Lemma: If p is prime with $p|ab$, then $p|a$ or $p|b$.
 - (h) Fundamental Theorem of Arithmetic
 - $n > 1$ is a product of primes in a unique way, except for rearranging factors.
 - There is a unique list of powers $s_1, s_2, s_3, \dots \geq 0$ with: $n = 2^{s_1} 3^{s_2} 5^{s_3} 7^{s_4} 11^{s_5} \dots$.
 - (i) Clock arithmetic: $a \equiv b \pmod{n}$ means $n|a-b$.

Methods of Proof: Examples

- Direct: $A \Rightarrow B$. Start with hypothesis A , deduce conclusion B .

Use: Whenever you can. This is the default method.

Proposition: For integers $a, b, c > 0$, if $a|b$ and $a|c$, then $a|(b+c)$.

Proof: Let $a|b$ and $a|c$, so $b = an$ and $c = am$. Then $b + c = an + am = a(n+m)$, so $a|(b+c)$.

- Cases: $(A \text{ and } C) \Rightarrow B$ and $(A \text{ and not } C) \Rightarrow B$.

Assume hypothesis A and take the case where C is true; deduce conclusion B .

Also, assume A and take the case where C is false; deduce B .

Use: When you need more information (C or not C) to get from A to B .

Proposition: For any integer n , we have $n^2 - n$ even.

Proof: There is no hypothesis other than $n \in \mathbb{Z}$. In case n is even, we have $n = 2m$ and $n^2 - n = 4m^2 - 2m = 2(2m^2 - m)$, which is even. In case n is not even (odd), we have $n = 2m + 1$ and $n^2 - n = 4m^2 + 4m + 1 - 2m - 1 = 2(2m^2 + m)$, which is also even.

- Contrapositive: $\text{not}(B) \Rightarrow \text{not}(A)$. Assume B is false, deduce A is false.

Use: When $\text{not}(B)$ is a simpler or more powerful assumption than A .

Proposition: For $a \in \mathbb{Z}$, if a^2 is even, then a is even.

Proof: Assume the contrapositive hypothesis that n is odd, that is $n = 2k+1$. Then $n^2 = 4k^2 + 4k + 1 = 2(2k^2+2k) + 1$. Thus n^2 is odd, which is the contrapositive conclusion.

- Contradiction: $(A \text{ and not } B) \Rightarrow (C \text{ and not } C)$.

Assume $A \Rightarrow B$ is false, meaning A is true and B is false. Deduce a contradiction, the impossible statement that C is both true and false.

Use: As last resort. You can't see why it's true, so you prove it can't be false.

Proposition: $\sqrt{2}$ is irrational

Proof: There is no hypothesis A , so we assume only $\text{not}(B)$: $\sqrt{2}$ is rational, meaning $\sqrt{2} = \frac{a}{b}$, a fraction in lowest terms. Then $2 = \frac{a^2}{b^2}$ and $a^2 = 2b^2$. Thus a^2 is even, and the previous result implies a is even, so that $a = 2m$. Hence $4m^2 = 2b^2$, and $2m^2 = b^2$, so b^2 is even, which implies b is even. However, since $\frac{a}{b}$ is in lowest terms and a is even, we must have b odd (otherwise the fraction could be reduced). That is, b is both even and odd (not even). This contradiction shows that our beginning assumption was false, and the Proposition is true.

To summarize: if you give me a fraction with $\frac{a}{b} = \sqrt{2}$, then I can produce an integer b which is both odd and even.

- Mathematical Induction: To prove $A(n)$ for all integers $n \geq b$:

Anchor (Base Case) $A(b)$; and Chain Step: for each $n \geq b$, $A(n) \Rightarrow A(n+1)$.

Use: When the statement $A(n)$ depends on an integer n , and $A(n)$ is part of $A(n+1)$.

Proposition: For all integers $n \geq 1$, we have $1 + 2 + 2^2 + \dots + 2^{n-1} = 2^n - 1$.

Proof: Anchor $A(1)$ says: $1 = 2^1 - 1$, which is true.

Chain: For some $n \geq 1$, assume the inductive hypothesis $A(n)$: $1 + 2 + 2^2 + \dots + 2^{n-1} = 2^n - 1$. Then $1 + 2 + 2^2 + \dots + 2^{n-1} + 2^n = (2^n - 1) + 2^n$ by the inductive hypothesis, which equals: $2(2^n) - 1 = 2^{n+1} - 1$. That is, we have $A(n+1)$: $1 + 2 + 2^2 + \dots + 2^n = 2^{n+1} - 1$, which is the inductive conclusion.

Final conclusion: $A(n)$ is true for all $n \geq 1$.

Problems

1. Relatively prime integers
 - (a) Prove: For $a, b \in \mathbb{Z}$, $\gcd(a, b) = 1 \iff na + mb = 1$ for some $n, m \in \mathbb{Z}$.
 - (b) Prove: For $a, b, c \in \mathbb{Z}$, if $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$, then $\gcd(a, bc) = 1$.
2. Suppose a positive integer n has the property: $n \mid ab \Rightarrow n \mid a$ or $n \mid b$. Then n is prime.
3. Recall the Fibonacci numbers $F_1 = F_2 = 1$, and $F_{n+1} = F_{n-1} + F_n$ for $n \geq 2$. Prove that for all $n \in \mathbb{N}$, we have $F_1 + F_2 + \cdots + F_n = F_{n+2} - 1$.
4. For positive integers a, b, c, d , if $ab \nmid cd$, then $a \nmid c$ or $b \nmid d$.
5. Let x be an irrational real number. Prove that either x^2 or x^3 is irrational.
6. PROP: For any $n \in \mathbb{N}$, at least one of the numbers $n, n+1, n+2, n+3$ is divisible by 4.
 - (a) Use induction to prove the Proposition.
 - (b) Use the Division Lemma to prove the Proposition.
7. Prove: Let $a_1 = 1$ and $a_{n+1} = \frac{1}{2}a_n + 1$ for $n \geq 1$. Then $a_n < 2$ for all n .
8. Prove: Let p, q be distinct primes. Then $\log_p(q)$ is irrational.
9. We get a commutative group from the real numbers \mathbb{R} with the addition operation, and also from the non-zero reals $\mathbb{R} \setminus \{0\}$ with the multiplication operation. Also, multiplication distributes over addition.

Give a fully detailed proof of the formula $(a+b)^2 = a^2 + 2ab + b^2$ for $a, b \in \mathbb{R}$, referring to the necessary axiom at each step.
10. Prove that 101 is prime.
11. Find all integer solutions (x, y) to the equation $13x + 5y = 1$.

Solutions

1a. PROP: For $a, b \in \mathbb{Z}$, we have $\gcd(a, b) = 1$ if and only if $na + mb = 1$ for some $n, m \in \mathbb{Z}$.

Proof: (\implies) Direct proof. If $\gcd(a, b) = 1$, then we know that the Euclidean Algorithm allows us to write $na + mb = \gcd(a, b) = 1$ for $m, n \in \mathbb{Z}$.

(\impliedby) Direct proof. Assume $na + mb = \gcd(a, b) = 1$ for $m, n \in \mathbb{Z}$. For any positive common divisor $c \mid a, b$, we have $c \mid na + mb = 1$, so $c = 1$. Thus, the greatest common divisor $\gcd(a, b) = 1$.

1b. PROP: For $a, b, c \in \mathbb{Z}$, if $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$, then $\gcd(a, bc) = 1$.

First Proof: Direct proof from previous results. Assume $\gcd(a, b) = \gcd(a, c) = 1$. By the Euclidean Algorithm, we can write $ma + nb = 1$ and $qa + rc = 1$, so that:

$$\begin{aligned} (1)(1) &= (ma + nb)(qa + rc) \\ &= (ma)(qa) + (nb)(qa) + (ma)(rc) + (nb)(rc) \\ &= (maq + nbq + mrc)a + (nr)(bc). \end{aligned}$$

That is, $ka + \ell(bc) = 1$ for $k, \ell \in \mathbb{Z}$, so Proposition 1(a) above gives $\gcd(a, bc) = 1$.

Second Proof. Contrapositive. Assume the contrapositive hypothesis: $d = \gcd(a, bc) > 1$. Then d has a prime factor $p \mid d$, with $p \mid a$ and $p \mid bc$. By the Prime Lemma, this means $p \mid b$, so that $\gcd(a, b) \geq p > 1$; or $p \mid c$, so that $\gcd(a, c) \geq p > 1$. In either case, $\gcd(a, b) > 1$ or $\gcd(a, c) > 1$, which is the contrapositive conclusion.

2. PROP: Let n be a positive integer such that $n \mid ab \implies n \mid a$ or $n \mid b$. Then n is prime.

Proof: The conclusion that n is prime is basically negative: n does *not* have a factorization. Thus, the contrapositive will be simpler to work with. The contrapositive hypothesis is that n is composite: $n = ab$ with $1 < a, b < n$. This gives some a, b with $n \mid ab$, but $n \nmid a$ and $n \nmid b$. This is precisely the contrapositive conclusion, the negation of $\forall a, b : n \mid ab \implies n \mid a$ or $n \mid b$.

3. PROP: The Fibonacci numbers F_n satisfy: $F_1 + F_2 + \cdots + F_n = F_{n+2} - 1$.

Proof. Induction. Let $A(n)$ be the formula for a given $n \geq 1$.

Base: $F_1 = 1 = 2 - 1 = F_3 - 1$, so $A(1)$ is true.

Chain. Assume $A(n)$: $F_1 + F_2 + \cdots + F_n = F_{n+2} - 1$ for some $n \geq 1$. Then:

$$\begin{aligned} F_1 + F_2 + \cdots + F_n + F_{n+1} &= (F_{n+2} - 1) + F_{n+1} && \text{by inductive hypothesis} \\ &= F_{n+2} + F_{n+1} - 1 = F_{n+3} - 1 && \text{by recurrence for } F_{n+3} \end{aligned}$$

which gives the inductive conclusion $A(n+1)$.

4. PROP: For positive integers a, b, c, d , if $ab \nmid cd$, then $a \nmid c$ or $b \nmid d$.

Proof. Contrapositive. Assume the contrapositive hypothesis $a \mid c$ and $b \mid d$. Then $c = na$ and $d = mb$, so that $cd = nmab$. This gives the contrapositive conclusion $ab \mid cd$.

5. Let x be an irrational real number. Prove that either x^2 or x^3 is irrational.

Proof. Contrapositive. Assume the contrapositive hypothesis x^2 and x^3 are rational, and $x \neq 0$. (The case $x = 0$ is obvious.) The the quotient of two rational numbers is rational, so $x = x^2/x^3$ is rational, which is the contrapositive hypothesis.

6. PROP: For any $n \in \mathbb{N}$, at least one of the numbers $n, n+1, n+2, n+3$ is divisible by 4.

a. Proof. Induction with cases. Base: Among 0,1,2,3, we have 0 divisible by 4.

Chain Step: Inductively assume 4 divides one of the numbers $n, n+1, n+2, n+3$. We wish to conclude that 4 divides one of the numbers $n+1, n+2, n+3, n+4$.

Case 1: If 4 divides one of $n+1, n+2, n+3$, then the conclusion holds. Case 2: If 4 divides n , then $n = 4k$ and $n+4 = 4(k+1)$ is divisible by 4, and the conclusion again holds.

b. Proof. Cases. Write $n = 4q + r$ for some $0 \leq r < 4$. Case 1: In case $r = 0$, then $n = 4q$, and $n+4 = 4(q+1)$ is divisible by 4. In case $r > 0$, let $k = 4 - r \in \{1, 2, 3\}$. Then $n+k = 4q+4 = 4(q+1)$ is divisible by 4, and $n+k$ is one of $n+1, n+2, n+3$. In either case, one of $n, n+1, n+2, n+3$ is divisible by 4.

7. PROP: Let $a_1 = 1$ and $a_{n+1} = \frac{1}{2}a_n + 1$ for $n \geq 1$. Then $a_n < 2$ for all n .

a. Proof. Induction. Base: $a_1 = 1 < 2$. Chain: Assume $a_n < 2$ for some n . Then $a_{n+1} = \frac{1}{2}a_n + 1 < \frac{1}{2}(2) + 1 = 2$. That is, $a_{n+1} < 2$.

8. PROP: Let p, q be distinct primes. Then $\log_p(q)$ is irrational.

Proof. Contradiction. Assume that $\log_p(q)$ is rational, meaning $\log_p(q) = a/b$ for integers a, b . We may assume $a, b > 0$ since the prime $q > 1$, so $\log_p(q) > 0$. Then $p^{\log_p(q)} = p^{a/b}$, so $q = p^{a/b}$, and $q^b = p^a$. By the Fundamental Theorem of Arithmetic, any integer has a unique factorization into primes, so it is not possible for q^a to be factored as p^b for a different prime p (remember $a, b > 0$). This contradiction proves our original assumption was false, meaning $\log_p(q)$ is irrational.

9. PROP: For any $a, b \in \mathbb{R}$, we have $(a + b)^2 = a^2 + 2ab + b^2$

Proof. Direct proof. Note that x^2 means $x \cdot x$ and 2 means $1+1$.

$$\begin{aligned}(a + b) \cdot (a + b) &= (a + b) \cdot a + (a + b) \cdot b && \text{by distributivity} \\ &= a \cdot a + b \cdot a + a \cdot b + b \cdot b && \text{by distributivity} \\ &= a \cdot a + a \cdot b + a \cdot b + b \cdot b && \text{by multiplicative commutativity} \\ &= a \cdot a + 1 \cdot a \cdot b + 1 \cdot a \cdot b + b \cdot b && \text{by multiplicative identity} \\ &= a \cdot a + (1+1) \cdot a \cdot b + b \cdot b && \text{by distributivity} \\ &= a^2 + 2 \cdot a \cdot b + b^2 && \text{by definition.}\end{aligned}$$

Also, we have used additive associativity throughout, which allows us to write expressions like $w + x + y + z$ without specifying which addition is done first, as in $((x + y) + z) + w$ or $(w + (x + y)) + z$.

10. PROP: 101 is a prime number.

Proof. We know that if n is composite, then n has a prime factor $p \leq \sqrt{n}$. Contrapositively, if n has no prime factor $p \leq \sqrt{n}$, then n is prime. Now, $n = 101$ is not divisible by $p = 2, 3, 5$, or 7 , since $\frac{101}{2} = 50\frac{1}{2}$, $\frac{101}{3} = 33\frac{2}{3}$, $\frac{101}{5} = 20\frac{1}{5}$, $\frac{101}{7} = 14\frac{3}{7}$. These are all the primes $p \leq \sqrt{101} \cong 10.05$, so 101 is prime.

11. To find all integer solutions to $13x + 5y = 1$, we first perform the Euclidean Algorithm on $a = 13$ and $b = 5$ (top-to-bottom), then perform back-substitution to get a particular solution to $13x + 5y = \gcd(13, 5)$ (bottom-to-top):

$$\begin{aligned}13 &= 2(5) + 3 & 1 &= -1(5) + 2(13 - 2(5)) = 2(13) - 5(5) \\ 5 &= 1(3) + 2 & 1 &= 1(3) - 1(5 - 3) = -1(5) + 2(3) \\ 3 &= 1(2) + 1 & 1 &= 3 - 1(2) = 1(3) - 1(2) \\ 2 &= 2(1) + 0\end{aligned}$$

Now from the particular solution $(2, -5)$, we get the general solution in terms of $d = \gcd(13, 5) = 1$: namely $(x, y) = (2 + \frac{5}{d}n, -5 - \frac{13}{d}n) = (2 + 5n, -5 - 13n)$ for all $n \in \mathbb{Z}$.