Unit 3 · Number Theory and Proof Cheat Sheet

Unit 3 focus: definitions, counterexamples, direct proof, existential and universal statements, rational numbers

1 DEFINITIONS TO USE

even	$n = 2k$ for some integer k	$-6 = 2(-3)$
odd	$n = 2k + 1$ for some integer k	$7 = 2(3) + 1$
rational	$r = a/b$, integers, $b \neq 0$	$0.75 = 3/4$
divides	$d \mid n$ means $n = dk$, k an integer	$3 \mid 12$
prime	$n > 1$ with divisors only 1, n	2, 3, 5, 7, 11
composite	$n > 1$ and not prime	$91 = 7 \cdot 13$

2 EXAMPLE VS PROOF

Goal	What is enough
prove “there exists …”	one example (a witness)
disprove “for all …”	one counterexample
prove “for all …”	a general argument with an arbitrary element
disprove “there exists …”	a general argument that nothing works

$n^2 + n + 41$ is prime for $n = 0, \ldots, 39$, but $n = 40$ gives 41^2: examples never prove “for all”.

3 DIRECT PROOF TEMPLATE

Suppose the hypothesis for an arbitrary element → **write** definitions → **algebra** → **conclude** with the definition.

Example: If m and n are odd, then mn is odd.
Suppose: $m = 2a + 1$, $n = 2b + 1$
Multiply: $mn = 4ab + 2a + 2b + 1$
Rewrite: $mn = 2(2ab + a + b) + 1$

Answer: mn **is odd since** $2ab + a + b$ **is an integer**

4 RATIONAL NUMBERS

Rationals are closed under $+, -, \times$ and $\div$ by nonzero numbers. Repeating decimals are rational.

Example: Write $x = 0.\overline{45}$ as a fraction.
Multiply: $100x = 45.\overline{45}$
Subtract: $99x = 45$, so $x = 45/99$

Answer: $\frac{5}{11}$

5 COUNTEREXAMPLES

“Every prime is odd.”	**2**
“$x^2 > x$ for every real x.”	$x = \frac{1}{2}$
“If $a \mid bc$ then $a \mid b$ or $a \mid c$.”	$6 \mid 2 \cdot 3$
“The product of irrationals is irrational.”	$\sqrt{2} \cdot \sqrt{2} = 2$

6 COMMON MISTAKES

✔ Do remember

- Use different letters for different numbers ($m = 2a$, $n = 2b$).
- Say why the factor is an integer.
- End with the definition you are proving.

✘ Common mistakes

- Proving with examples: use an arbitrary element
- $(2k + 1)^2 = 4k^2 + 1$: it is $4k^2 + 4k + 1$
- Assuming what you want to prove: that is circular

Unit 3 · Number Theory and Proof Cheat Sheet

More practice: divisibility, the quotient-remainder theorem, proof by contradiction and contraposition, choosing a strategy

1 QUOTIENT-REMAINDER THEOREM

For any integer n and $d > 0$ there are unique q, r with $n = dq + r$ and $0 \le r < d$.

Example: $n = -17$, $d = 5$
Choose q: $q = -4$ (not -3)
Check: $5(-4) + 3 = -17$

Answer: $q = -4$, $r = 3$

2 DIVISIBILITY FACTS

Fact	Why
$a \mid b$ and $b \mid c \Longrightarrow a \mid c$	$c = bs = a(rs)$
$a \mid b$ and $a \mid c \Longrightarrow a \mid (xb + yc)$	$xb + yc = a(xr + ys)$
$n(n+1)$ is even	one of two consecutive integers is even
$\gcd(252, 198) = 18$	Euclid: $252 = 198 + 54$, $198 = 3 \cdot 54 + 36$, $54 = 36 + 18$, $36 = 2 \cdot 18$

3 PROOF BY CONTRADICTION

Assume the statement is **false**; reason until you reach something impossible.

Example: Prove $\sqrt{2}$ is irrational.
Assume: $\sqrt{2} = a/b$ in lowest terms
Then: $a^2 = 2b^2$, so a is even, $a = 2k$
Then: $b^2 = 2k^2$, so b is even too

Answer: Contradiction: a/b was not in lowest terms

4 PROOF BY CONTRAPOSITION

To prove $p \to q$, prove $\neg q \to \neg p$ (they are equivalent).

Example: If n^2 is even, then n is even.
Contrapositive: if n is odd, n^2 is odd
Proof: $n = 2k + 1 \Longrightarrow n^2 = 2(2k^2 + 2k) + 1$

Answer: proved

5 CHOOSING A STRATEGY

Statement looks like …	Try
“There is …”	give a witness
“For all …” with usable definitions	direct proof
“There is no …”, “… is irrational”, “infinitely many”	contradiction
“If n^2 …, then n …”	contraposition
finite domain	exhaustion (check every case)
false “for all”	counterexample

6 CHALLENGE: INFINITELY MANY PRIMES

Suppose the primes were only $p_1, p_2, \ldots, p_n$. Let $N = p_1 p_2 \cdots p_n + 1$. Some prime p divides N. It must be one of the p_i, so p divides $N - p_1 \cdots p_n = 1$ — impossible. So there are infinitely many primes. (N itself need not be prime: $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$.)