Disc Math - §5 - Some proof techniques

We want to prove facts that are not universally true, but only in some context (Calculus, Algebra, Number Theory, Graph Theory) =
→ we introduce Axioms = Additional Hypothesis. Now not every statement which is true in a context is necessarily provable. Any system (of axioms) containing elementary arithmetic is not complete.

Theorems in subject-specific context are usually proved less formally then in pure predicate logic. Eg. instead of $\forall x, P(x) \to Q(x)$ we prove $P(x) \to Q(x)$.

Inductive reasoning → drawing a conclusion based on experience

Deductive reasoning → produce a logical proof or find a counterexample.

① Counterexample: One counterexample is enough to disprove a conjectured Theorem:

Ex: $n! \le n^3$, $n \ge 1$: $1! = 1^3$; $2! = 2 \le 2^3 = 8$; $3! = 6 \le 3^3 = 27$;

$4! = 24 \le 4^3 = 64$, $5! = 120 \le 5^3 = 125$; $6! = 720 \ge 6^3 = 216$ (Done.)

② Exhaustive proof.

Ex: $n! \le n^3$, $1 \le n \le 5$ Proved above.

$n! \le n^3$, $0 \le n \le 5$ Disproven by $0! = 1 \ge 0^3 = 0$.

③ Direct proof.

Ex: Prove that the product of an even integer and an integer is even

$$\frac{\dfrac{x \in \mathbb{Z}_{even}}{\exists z \in \mathbb{Z} \text{ s.t. } x = 2z}}{\dfrac{xy = (2z)y = 2(zy)}{xy \in \mathbb{Z}_{even}}}$$

Thus $\dfrac{x \in \mathbb{Z}_{even} \to xy \in \mathbb{Z}_{even}}{\forall x \in \mathbb{Z}, \forall y \in \mathbb{Z}, x \in \mathbb{Z}_{even} \to xy \in \mathbb{Z}_{even}}$ ug

Disc Math - §5 - Some proof techniques

Of course, we usually write this as:

Let $x = 2z$ be an even integer and let y be an integer. Then $xy = 2(zy)$ is an even integer.

Ex: Prove that if $10|u$ and $12|m$, $u, m \in \mathbb{Z}$ then $15 \mid um$.

Pr: $u = 10k$, $m = 12\ell \Rightarrow um = 10 \cdot 12 \cdot k\ell = (5\cdot 2)(3\cdot 4)k\ell = 15(8k\ell)$,

④ Proof by contrapositive. Prove $Q' \to P'$ instead of $P \to Q$.

Ex: $\forall u \in \mathbb{Z}$, $u^2 \in \mathbb{Z}_{even} \to u \in \mathbb{Z}_{even}$. Prove instead $\forall u \in \mathbb{Z}$, $u \notin \mathbb{Z}_{even} \to u^2 \notin \mathbb{Z}_{even}$, i.e. $\forall u \in \mathbb{Z}$, $u \in \mathbb{Z}_{odd} \to u^2 \in \mathbb{Z}_{odd}$.

$u = 2k+1 \to u^2 = 2(2k^2+2k)+1 \in \mathbb{Z}_{odd}$. ☒

rem: $u, m \in \mathbb{Z}$. Then $u \bmod m = r$ if $u = mq + r$, $q, r \in \mathbb{Z}$, $0 \le r < m$

e.g. $7 \bmod 3 = 1$; $3 \bmod 7 = 3$; $-11 \bmod 4 = 1$; $-7 \bmod 3 = 2$

Ex: If $u \in \mathbb{N}$ s.t. $u \bmod 4 = 2$ or 3, then u is not a perfect square.

Sol: We will prove the contrapositive: If $u \in \mathbb{N}$ is a perfect square then $u \bmod 4 = 0$ or 1.

cases: Suppose $u = k^2$. If $k = 2\ell \in \mathbb{Z}_{even}$, $u = (2\ell)^2 = 4\ell^2 \to u \bmod 4 = 0$

If $k = (2p+1)$ then $u = k^2 = (2p+1)^2 = 4p^2+4p+1 \to u \bmod 4 = 1$. ☒

rem: Remember that $P \to Q$ and its converse $Q \to P$ are not equivalent

Ex: Prove that for two integers m, u their product mu is odd iff both m and u are odd.

Pr: $m, u \in \mathbb{Z}_{odd} \to (mu) \in \mathbb{Z}_{odd}$: $m = 2k+1$, $u = 2\ell+1 \to mu = 4k\ell + 2k + 2\ell + 1 \in \mathbb{Z}_{odd}$

$(mu) \in \mathbb{Z}_{odd} \to m, u \in \mathbb{Z}_{odd}$, prove the contrapositive $m, u \in \mathbb{Z}_{even} \to mu \in \mathbb{Z}_{even}$

: $m = 2k$, $u = 2\ell \to mu = 4k\ell \in \mathbb{Z}_{even}$.

⑤ Prove by contradiction. $(P \wedge Q' \to 0) \leftrightarrow (P \to Q)$ is a tautology (truth table). So to prove $P \to Q$ it is sufficient to prove $P \wedge Q' \to 0$. special case: $Q' \to 0 \equiv Q$

Lm: $\forall u \in \mathbb{Z}$, $\forall$ prime p if $p \mid u$ then $p \nmid (u+1)$.

Pr: By contradiction. Suppose $\exists u \in \mathbb{Z}$ s.t. $\exists p$-prime s.t. $p \mid u \wedge p \mid u+1$.

Thus $u = pr$, $u+1 = ps \rightarrow (u+1) - u = 1 = p(s-r) \rightarrow p \mid 1$. Contradict ☒

Th: The set of all primes is infinite. (Euclid 300 BC).

Pr: By contradiction. Suppose that the set of primes is finite; list them in ascending order: $2, 3, 5, 7, 11, \ldots, p$.

Let $N = (2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \ldots p) + 1$. Then, N is divisible by some prime q.

But by construction $q \mid N - 1$. By the previous Lemma we have a contradiction. ☒

rem: → Mersenne primes $2^p - 1$, p-prime (not all p work).

→ Fermat primes $2^{2^n} + 1$ (again not all n work).

---

rem: Recall that $x \in \mathbb{Q}$ means $x = p/q$, $p, q \in \mathbb{Z}$, $q \neq 0$.

Th: $\sqrt{2} \notin \mathbb{Q}$ (Pythagoras 500 BC)

Pr: By contradiction. Assume $\sqrt{2} = p/q$, $p, q \in \mathbb{Z}$, no common factor.

$2q^2 = p^2 \rightarrow 2 \mid p^2 \rightarrow 2 \mid p \rightarrow p = 2k \rightarrow 2q^2 = 4k^2$ i.e. $q^2 = 2k^2$

$\rightarrow 2 \mid q^2 \rightarrow 2 \mid q$ Contradiction. ☒

rem: $\sqrt{3} \notin \mathbb{Q}$, $\sqrt{3} = \frac{m}{n}$, $3n^2 = m^2 \rightarrow 3 \mid m \rightarrow 3n$. Contradiction.

? $\sqrt{4}, \sqrt{6}, \sqrt{8}, \sqrt{10}, 3\sqrt{5}, \ldots$

Ex: The sum of a rational number and an irrational number is irrational.

Pr: By contradiction. Suppose $r \in \mathbb{Q}$, $r = \frac{a}{b}$; $s \notin \mathbb{R} \setminus \mathbb{Q}$ and $r + s = \frac{c}{d} \in \mathbb{Q}$, $a, b, c, d \in \mathbb{Z}$, $b \neq 0$, $d \neq 0$. Then

$$s = \frac{c}{d} - \frac{a}{b} = \frac{bc - ad}{bd} \in \mathbb{Q}.$$ Contradiction. ☒

HW §2.1 p107: 10, 22, 30, 32, 38, 45, 46, 60, 68, 71