Vorlesung

Logik und Diskrete Mathematik

(Mathematik für Informatiker I)

Wintersemester 2008/09

FU Berlin
Institut für Informatik

Klaus Kriegel

Literatur zur Vorlesung:

C. Meinel, M. Mundhenk, Mathematische Grundlagen der Informatik, B.G.Teubner 2000

G. Haggard, J. Schlipf, S. Whitsides, Discrete Mathematics for Computer Science, Brooks Cole

U. Schöning, Logik für Informatiker, Spektrum, 1987

M. Aigner, Diskrete Mathematik, Vieweg & Sohn 1999

D. Hachenberger, Mathematik fr Informatiker, Pearson Studium

T. Ihringer, Diskrete Mathematik, Teubner 1994

K. H. Rosen, Discrete Mathematics and its Applications, McGraw-Hill 1991

R. L. Graham, D. E. Knuth, O. Patashnik, Concrete Mathematics, Addison-Wesley 1994

C. L. Liu, Elements of Discrete Mathematics, McGraw-Hill

1 Einführung: Grundbegriffe der Logik

1.1 Aussagen

Die klassische Aussagenlogik beruht auf zwei Grundprinzipien, dem *Zweiwertigkeitsprinzip*, welches fordert, dass jede Aussage einen eindeutig bestimmten Wahrheitswert hat, der nur *wahr* oder *falsch* sein kann, und dem *Extensionalitätsprinzip*, nach dem der Wahrheitswert einer zusammengesetzten Aussage nur von den Wahrheitswerten ihrer Bestandteile abhängt.
Wir werden im folgenden eine 1 für den Wahrheitswert *wahr* und eine 0 für *falsch* verwenden. Das Zusammensetzen von Aussagen erfolgt durch die Verwendung von Verknüpfungswörtern wie *und, oder, nicht, wenn ... dann.*

Definition: Eine Aussage ist ein Satz (ein formalsprachliches Gebilde), das entweder wahr oder falsch ist.

Beispiele:

1. Der Satz *"7 ist eine Primzahl."* und der Satz *"7 ist eine ungerade Zahl."* sind wahre Aussagen. Dagegen ist der Satz *"7 ist eine gerade Zahl."* eine falsche Aussage. Genauer gesehen ist der letzte Satz die Negation des zweiten Satzes, denn *nicht ungerade* zu sein, ist (zumindest für ganze Zahlen) das gleiche, wie *gerade* zu sein.

2. Der Satz *"7 ist eine Primzahl und 7 ist ungerade."* sowie der Satz *"7 ist eine Primzahl oder 7 ist gerade."* sind wahre Aussagen. Achtung: Auch der Satz *"7 ist eine Primzahl oder 7 ist ungerade."* ist eine wahre Aussage, denn das logische *oder* ist kein ausschließendes *entweder oder*. Dagegen ist der Satz *"7 ist eine Primzahl und 7 ist gerade."* eine falsche Aussage, denn die zweite Aussage ist falsch.

3. Der Satz *"$\sqrt{2}$ ist eine rationale Zahl."* ist – wie man aus der Schulmathematik weiß – eine falsche Aussage, aber es bedarf schon einiger Überlegungen, um das zu zeigen.

4. Der Satz *"Jede gerade natürliche Zahl größer als* 2 *ist die Summe zweier Primzahlen"* ist eine Aussage, denn entweder es gibt eine gerade Zahl, die sich nicht als Summe zweier Primzahlen darstellen lässt (dann ist die Aussaage falsch), oder es gibt keine solche Zahl (dann ist die Aussage wahr). Man nimmt an, dass die Aussage wahr ist (Goldbach Vermutung), konnte das aber bisher noch nicht beweisen.

5. Der Satz *"Dieser Satz ist falsch."* ist als Russels Paradoxon bekannt. Durch die spezielle Art des Bezugs auf sich selbst kann er weder wahr noch falsch sein und ist deshalb **keine** Aussage.

Wie wir in Punkt zwei gesehen haben, bestimmt sich der Wahrheitswert einer zusammengesetzten Aussage ausschließlich aus den Wahrheitswerten der Ausgangskomponenten. Deshalb ist es sinnvoll, Aussagevariablen einzuführen und die Wahrheitwerte

von zusammengestezten Aussagen durch sogenannte Wahrheitsswerttabellen (kurz Wahrheitstafeln) zu beschreiben. Die Negation einer Aussage p wird mit $\neg(p)$ bezeichnet. Diese Operation kehrt den Wahrheitswert von p um, d.h. man kann sie als Wahrheitswertfunktion $\neg : \{0,1\} \longrightarrow \{0,1\}$ mit $\neg(0) = 1$ und $\neg(1) = 0$. Analog können Verknüpfungen von zwei Aussagen p und q, wie

die *Konjunktion* $p \wedge q$ (gesprochen "*p und q*"),
die *Disjunktion* $p \vee q$ (gesprochen "*p oder q*"),
die *Implikation* $p \rightarrow q$ (gesprochen "*aus p folgt q*"),
die *Äquivalenz* $p \leftrightarrow q$ (gesprochen "*p genau dann wenn q*"),
die *Antivalenz* $p \oplus q$ (gesprochen "*entweder p oder q*")

durch Funktionen von $\{0,1\} \times \{0,1\}$ nach $\{0,1\}$ charakterisiert werden. Die folgende Tabelle enthält die Definition dieser 5 Funktionen:

p	q	$p \wedge q$	$p \vee q$	$p \rightarrow q$	$p \leftrightarrow q$	$p \oplus q$
0	0	0	0	1	1	0
0	1	0	1	1	0	1
1	0	0	1	0	0	1
1	1	1	1	1	1	0

Aus der Tabelle kann man ablesen, dass die Konjunktion $p \wedge q$ dann und nur dann wahr ist, wenn beide Aussagen p und q wahr sind. Die Disjunktion $p \vee q$ ist dann und nur dann wahr, wenn mindestens eine der Aussagen p und q wahr ist. Die Implikation ist dann und nur dann wahr, wenn p falsch oder q wahr ist. Versuchen Sie selbst, die Äquivalenz und die Antivalenz verbal zu beschreiben!

Ausdrücke, die durch (wiederholtes) Anwenden der Verknüpfungsoperationen aus Variablen gewonnen werden, nennt man *Formeln* (oder *Terme*) der Aussagenlogik. Um eine Formel eindeutig erkennen zu können, müsste man jeweils nach Anwendung einer Verknüpfung die neue Formel durch ein Klammerpaar einschließen. Weil die Formeln dadurch aber sehr unübersichtlich werden können, vereinbart man einige Regeln zur Vereinfachung der Notation (ähnlich wie die bekannte Regel, dass Punktrechnung vor Strichrechnung geht):

- Außenklammern können weggelassen werden.
- In der Reihenfolge $\neg, \wedge, \vee, \rightarrow, \leftrightarrow$ trennen die hinteren Junktoren (Verknüpfungssymbole) stärker als alle vorangehenden, d.h. die Bindungsstärke nimmt in dieser Reihenfolge ab. Klammerungen, die mit dieser Hierarchie der Bindungsstärke übereinstimmen, können weggelassen werden.

Man kann also $((\neg p_1) \vee (p_2 \wedge p_3))$ auch $\neg p_1 \vee p_2 \wedge p_3$ schreiben. Dagegen würde das Weglassen der Klammern in der Formel $\neg(p \vee q)$ eine andere Formel erzeugen.

Legt man für alle in einer Formel auftretenden Variablen Wahrheitswerte fest, so induziert eine solche Belegung auch einen Wahrheitswert für die Formel. Man nennt

diesen induktiven Prozess auch *Auswertung* der Formel. Die Ergebnisse der Auswertungen einer Formel unter allen möglichen Belegungen werden in einer Wahrheitstafel zusammengefasst.

Definition: Zwei Formeln α und β sind *logisch äquivalent*, wenn jede beliebige Belegung der Variablen für beide Formeln den gleichen Wahrheitswert induziert. Wir schreiben dafür $\alpha \equiv \beta$.

Wie das folgende Beispiel zeigt, kann die Äquivalenz von zwei Formeln prinzipiell durch Wahrheitstafeln überprüft werden: Man stelle fest, ob die Formeln
$\alpha = \neg(p_1 \vee ((p_1 \vee p_2) \wedge p_2)$ und $\beta = \neg p_1 \wedge \neg p_2$ logisch äquivalent sind!

p_1	p_2	$p_1 \vee p_2$	$(p_1 \vee p_2) \wedge p_2$	$p_1 \vee ((p_1 \vee p_2) \wedge p_2)$	α
0	0	0	0	0	1
0	1	1	1	1	0
1	0	1	0	1	0
1	1	1	1	1	0

p_1	p_2	$\neg p_1$	$\neg p_2$		β
0	0	1	1		1
0	1	1	0		0
1	0	0	1		0
1	1	0	0		0

Wie man sieht, ist der Wahrheitswerteverlauf für α und β identisch, die Formeln sind also äquivalent.

Satz: Für beliebige Formeln α, β, γ gelten die folgenden Äquivalenzen:

Assoziativität:	$(\alpha \wedge \beta) \wedge \gamma$	$\equiv$	$\alpha \wedge (\beta \wedge \gamma)$
	$(\alpha \vee \beta) \vee \gamma$	$\equiv$	$\alpha \vee (\beta \vee \gamma)$
Kommutativität:	$\alpha \wedge \beta$	$\equiv$	$\beta \wedge \alpha$
	$\alpha \vee \beta$	$\equiv$	$\beta \vee \alpha$
Distributivität:	$\alpha \wedge (\beta \vee \gamma)$	$\equiv$	$(\alpha \wedge \beta) \vee (\alpha \wedge \gamma)$
	$\alpha \vee (\beta \wedge \gamma)$	$\equiv$	$(\alpha \vee \beta) \wedge (\alpha \vee \gamma)$
Idempotenz:	$\alpha \wedge \alpha$	$\equiv$	α
	$\alpha \vee \alpha$	$\equiv$	α
Dominanz:	$\alpha \wedge 0$	$\equiv$	0
	$\alpha \vee 1$	$\equiv$	1
Identität:	$\alpha \wedge 1$	$\equiv$	α
	$\alpha \vee 0$	$\equiv$	α
Absorbtion:	$\alpha \wedge (\alpha \vee \beta)$	$\equiv$	α
	$\alpha \vee (\alpha \wedge \beta)$	$\equiv$	α
deMorgansche Regel:	$\neg(\alpha \wedge \beta)$	$\equiv$	$\neg\alpha \vee \neg\beta$
	$\neg(\alpha \vee \beta)$	$\equiv$	$\neg\alpha \wedge \neg\beta$
Komplementierung:	$\alpha \wedge \neg\alpha$	$\equiv$	0
	$\alpha \vee \neg\alpha$	$\equiv$	1
(doppelte Negation)	$\neg\neg\alpha$	$\equiv$	α

Diese Äquivalenzen können leicht mit Wahrheitstafeln bewiesen werden. Der Wahrheitstafelmethode sind jedoch enge Grenzen gesetzt, wenn die Anzahl n der verwendeten Variablen groß wird, denn die entsprechende Wahrheitstafel hat dann 2^n Zeilen.

Beispiel: Der Beweis der folgenden Äquivalenz mit Wahrheitstafeln würde 16 Zeilen erfordern. Verwendet man dagegen die Absorbtion und die doppelte Negation zur Ersetzung von Subformeln, so erhält man einen einfachen und kurzen Beweis.

$$\begin{aligned} p_1 \vee ((p_2 \vee p_3) \wedge \neg(\neg p_1 \wedge (\neg p_1 \vee p_4))) &\equiv p_1 \vee ((p_2 \vee p_3) \wedge \neg\neg p_1) \\ &\equiv p_1 \vee ((p_2 \vee p_3) \wedge p_1) \\ &\equiv p_1 \end{aligned}$$

Die folgende Liste enthält weitere Äquivalenzen, welche zum Beweis der Äquivalenz von komplexen Formeln häufig angewendet werden:

$$\begin{array}{lrcl} (1) & \alpha \to \beta & \equiv & \neg\alpha \vee \beta \\ (2) & \alpha \leftrightarrow \beta & \equiv & \alpha \wedge \beta \vee \neg\alpha \wedge \neg\beta \\ (3) & \alpha \to \beta \wedge \gamma & \equiv & (\alpha \to \beta) \wedge (\alpha \to \gamma) \\ (4) & \alpha \to \beta \vee \gamma & \equiv & (\alpha \to \beta) \vee (\alpha \to \gamma) \\ (5) & \alpha \wedge \beta \to \gamma & \equiv & (\alpha \to \gamma) \vee (\beta \to \gamma) \\ (6) & \alpha \vee \beta \to \gamma & \equiv & (\alpha \to \gamma) \wedge (\beta \to \gamma) \end{array}$$

Definition: Eine Formel α wird erfüllbar genannt, wenn es eine Belegung der Variablen von α gibt, die für α den Wert 1 induziert. Die Formel α wird *allgemeingültig, logisch gültig* oder eine *Tautologie* genannt, wenn sie für jede Belegung den Wert 1 annimmt. Eine Formel, die unerfüllbar ist, wird *Kontradiktion* genannt.

1.2 Prädikate und Quantoren

Definition: Ein *Prädikat* ist eine Aussageform, die eine (oder mehrere) Variable enthält, so dass bei Ersetzung der Variablen durch Elemente aus einem gegebenen Individuenbereich U eine Aussage mit eindeutig bestimmten Wahrheitswert entsteht, z.B. "$x = 0$" oder "$x + 0 = x$" oder "$x + y = x$" für den Bereich der ganzen Zahlen.

Die Belegung der Variablen durch konkrete Objekte ermöglicht somit (durch Betrachtung eines Spezialfalls), ein Prädikat in eine Aussage umzuwandeln.
Sogenannte Quantoren erlauben es, aus diesen Spezialfällen allgemeinere Aussagen abzuleiten: Durch das Hinzufügen der Wendungen "für alle ...", symbolisch durch den Allquantor $\forall$, oder "es gibt ein ...", symbolisch durch den Existenzquantor $\exists$, werden die Variablen in einem Prädikat gebunden. Sind alle Variablen eines Prädikats gebunden, entsteht eine Aussage, also ein Satz, der wahr oder falsch ist.

Die Ausssage "$\forall x \in U \quad P(x)$" ist wahr, wenn für jedes Element $a \in U$ die Aussage $P(a)$ wahr ist. Dagegen ist "$\exists x \in U \quad P(x)$" eine wahre Aussage, wenn (mindestens) ein Element $a \in U$ existiert, so dass die Aussage $P(a)$ wahr ist.

Beispiele: Die Aussagen "$\forall x \in \mathbb{N} \quad x + 0 = x$" und "$\exists x \in \mathbb{N} \quad x^2 = x$" sind wahr, die Aussagen "$\exists x \in \mathbb{N} \quad x + 1 = x$" und "$\forall x \in \mathbb{N} \quad x^2 = x$" sind falsch.

Satz: Für beliebige Prädikate $P(x), Q(x)$ und $R(x, y)$ gelten die folgenden Äquivalenzen:

$$\begin{aligned}
\neg\forall x\ P(x) &\equiv \exists x \neg P(x) \\
\neg\exists x\ P(x) &\equiv \forall x \neg P(x) \\
\forall x\ P(x) \wedge \forall x\ Q(x) &\equiv \forall x\ (P(x) \wedge Q(x)) \\
\exists x\ P(x) \vee \exists x\ Q(x) &\equiv \exists x\ (P(x) \vee Q(x)) \\
\forall x \forall y\ R(x, y) &\equiv \forall y \forall x\ R(x, y) \\
\exists x \exists y\ R(x, y) &\equiv \exists y \exists x\ R(x, y)
\end{aligned}$$

Achtung: Die folgenden Formelpaare sind im allgemeinen nicht äquivalent:

$$\begin{array}{lll}
(\forall x\ P(x) \vee \forall x\ Q(x)) & \textit{und} & \forall x\ (P(x) \vee Q(x)) \\
(\exists x\ P(x) \wedge \exists x\ Q(x)) & \textit{und} & \exists x\ (P(x) \wedge Q(x)) \\
\forall x \quad (\exists y\ R(x, y)) & \textit{und} & \exists y \quad (\forall x\ R(x, y))
\end{array}$$

Konkrete Gegenbeispiele für das erste und zweite Paar erhält man für den Bereich der ganzen Zahlen wenn $P(x)$ (bzw. $Q(x)$) aussagt, daß x eine gerade (bzw. ungerade) Zahl ist. Für das dritte Paar kann man das Prädikat $R(x, y) = 1 \iff x \leq y$ über den reellen Zahlen verwenden.

1.3 Beweistechniken

In diesem Abschnitt geht es darum, einige grundlegende Beweisstrategien kennenzulernen. Da das prinzipielle Verständnis im Mittelpunkt stehen soll, sind die in den Beispielen bewiesenen Aussagen sehr einfach gewählt. Gerade bei diesen scheinbaren Selbstverständlichkeiten wird ein weiteres Problem deutlich: Bevor man an einen Beweis geht, muss man sich klarmachen, was man schon als Basiswissen voraussetzen kann, und was man noch beweisen muss. Oft ist als erster hilfreicher Schritt eine geeignete Formalisierung der Aussage notwendig.

Viele mathematische Sätze haben die Form einer Implikation, sie sagen, dass aus einer bestimmten Voraussetzung p eine Behauptung q folgt. Zum Beweis kann man verschiedene Techniken anwenden. Basis für die Gültigkeit solcher Beweise sind einige einfache Äquivalenzen und Implikationen, die man leicht mit der Wahrheitstafelmethode nachweisen kann. Die naheliegendste Technik ist der *direkte Beweis*, der darauf beruht, die Implikation $p \to q$ in mehrere elementare Teilschritte zu zerlegen, wobei man die folgende Tautologie nutzt: $((p \to r) \wedge (r \to q)) \to (p \to q)$. Wie das folgende Beispiel zeigt, bewegt man sich bei der Begründung der Elementarschritte in einem System, das sich auf einigen Axiomen (Grundannahmen) aufbaut und in dem man auf bereits bewiesene Tatsachen zurückgreifen kann.

Satz: Ist eine natürliche Zahl n durch 6 teilbar, so ist ihr Quadrat durch 9 teilbar.

Beweis: Die Idee ist offensichtlich – ist n durch 6 teilbar, so kann man den Faktor 6 und damit auch den Faktor 3 von n abspalten. Folglich kann man den Faktor 3

mindestens zwei mal von n^2 abspalten. Wenn wir diese Idee etwas formaler umsetzen wollen, müssen wir mit der Definition von Teilbarkeit beginnen:
$n \in \mathbb{N}$ ist durch $k \in \mathbb{N}$ teilbar, falls ein $l \in \mathbb{N}$ existiert, so dass $n = k \cdot l$.
Damit kann man die Voraussetzung des Satzes durch eine einfache Formel ausdrücken und die folgende Beweiskette bilden:

n ist durch 6 teilbar		Hypothese
$\exists l \in \mathbb{N}$	$n = 6 \cdot l$	Teilbarkeitsdefinition
$\exists l \in \mathbb{N}$	$n = (3 \cdot 2) \cdot l$	$6 = 3 \cdot 2$
$\exists l \in \mathbb{N}$	$n^2 = ((3 \cdot 2) \cdot l)((3 \cdot 2) \cdot l)$	Quadrieren
$\exists l \in \mathbb{N}$	$n^2 = (3 \cdot 3)((2 \cdot 2) \cdot (l \cdot l))$	Muliplikation ist assoziativ und kommutativ
$\exists l \in \mathbb{N}$	$n^2 = 9 \cdot (4 \cdot l^2)$	$3 \cdot 3 = 9$ und $2 \cdot 2 = 4$
$\exists l' \in \mathbb{N}$	$n^2 = 9 \cdot l'$	$l' = 4l^2$
n^2 ist durch 9 teilbar		Teilbarkeitsdefinition

Genau betrachtet haben wir beim Schritt von der vierten zur fünften Zeile sogar mehrere Elementarschritte zu einem Schritt zusammengefasst.

Manchmal ist es schwierig, den Beweis direkt zu führen. Als Alternativen bieten sich indirekte Beweise durch Kontraposition oder in der Form von Widerspruchs-Beweisen an. Beim *Beweis durch Kontraposition* wird anstelle von $p \to q$ die logisch äquivalente Aussage $\neg q \to \neg p$ bewiesen. Beim Widerspruchs-Beweis wird an Stelle von $p \to q$ die logisch äquivalente Aussage $(p \wedge \neg q) \to 0$ bewiesen. Wir demonstrieren beide Beweisverfahren an einfachen Beispielen.

Satz: Für jede natürliche Zahl n gilt: Ist n^2 ungerade, so ist auch n ungerade.

Beweis durch Kontraposition: Da die Negation von *"ungerade sein"* die Eigenschaft *"gerade sein"* ist, lautet die Kontraposition *" Ist n gerade, so ist auch n^2 gerade"*. und dafür gibt es einen einfachen direkten Beweis:
Ist n gerade, so gibt es eine ganze Zahl k mit $n = 2k$. Folglich ist $n^2 = (2k)^2 = 2 \cdot (2k^2)$ und somit ist n^2 gerade.

Satz: Für jede natürliche Zahl n gilt: Ist $\sqrt{n}$ keine ganze Zahl, dann ist $\sqrt{n}$ auch nicht rational.

Beweis durch Widerspruch: Man geht von der Annahme aus, dass $\sqrt{n}$ keine natürliche Zahl, aber eine rationale Zahl ist, und muss daraus einen Widerspruch ableiten. Sei $n = p_1^{k_1} \cdot \ldots \cdot p_l^{k_l}$ die eindeutige Primzahlzerlegung von n, wobei $p_1, \ldots, p_l$ die paarweise verschiedenen Primfaktoren von n sind und $k_1, \ldots, k_l$ die Vielfachheiten dieser Primfaktoren. Wären alle Werte $k_1, \ldots, k_l$ gerade Zahlen, dann wäre $\sqrt{n}$ eine ganze Zahl, nämlich $p_1^{k_1/2} \cdot \ldots \cdot p_l^{k_l/2}$. Nach unserer Annahme muss also mindestens einer dieser Werte ungerade sein, oBdA. (d.h. ohne Beschränkung der Allgemeinheit) sei das k_1.
Darüber hinaus soll $\sqrt{n}$ rational, also als Quotient aus zwei natürlichen Zahlen m und m' darstellbar sein. Damit ist $n = \left(\frac{m}{m'}\right)^2$ und $n \cdot m'^2 = m^2$. Kombiniert man diese Gleichung mit den Primzahlzerlegungen von $m = q_1^{i_1} \cdot \ldots \cdot q_j^{i_j}$ und $m' = r_1^{i'_1} \cdot \ldots \cdot r_{j'}^{i'_{j'}}$,

ergibt sich:

$$p_1^{k_1} \cdot \ldots \cdot p_l^{k_l} \cdot r_1^{2i'_1} \cdot \ldots \cdot r_{j'}^{2i'_{j'}} = q_1^{2i_1} \cdot \ldots \cdot q_j^{2i_j}.$$

Folglich tritt der Primfaktor p_1 auf der linken Seite in ungerader Vielfachheit auf und auf der rechten Seite in gerader Vielfachheit (unabhängig davon, ob p_1 überhaupt in m oder m' vorkommt). Das ist aber ein Widerspruch zur eindeutigen Primzahlzerlegung von natürlichen Zahlen.

Häufig ist es notwendig, verschiedene Fälle zu analysieren. Das dabei verwendete logische Prinzip ist Äquivalenz der Aussagen $p \to q$ und $(p \wedge r \to q) \wedge (p \wedge \neg r \to q)$, wir unterscheiden also die Fälle r und $\neg r$.

Beispiel: Wir beweisen durch Fallunterscheidung, das für jede Primzahl $p \geq 5$ die Zahl $p^2 - 1$ durch 24 teilbar ist.
Zuerst formen wir $p^2 - 1$ in $(p+1)(p-1)$ um und beobachten, dass von drei aufeinanderfolgenden ganzen Zahlen genau eine 3 teilbar ist. Da $p > 3$ und Primzahl ist, muss $p - 1$ oder $p + 1$ und damit auch $p^2 - 1$ durch 3 teilbar sein. Bleibt zu zeigen, dass $p^2 - 1$ durch 8 teilbar ist. Da p ungerade ist sind sowohl $p - 1$ als auch $p + 1$ gerade und damit ist $p^2 - 1$ durch 4 teilbar. Den noch fehlenden Faktor 2 kann man durch Fallunterscheidung nachweisen:
1. Fall: Ist $p - 1$ durch 4 teilbar, so ist $p - 1 = 4k$ und $p + 1 = 4k + 2 = 2(2k + 1)$ und damit $p^2 - 1 = 8k(2k + 1)$ für eine natürliche Zahlen k.
2. Fall: Ist $p - 1$ nicht durch 4 teilbar, so hat es die Form $4m + 2 = 2(2m + 1)$ für eine natürliche Zahl m und folglich ist $p + 1 = 4m + 4 = 4(m + 1)$. Damit erhalten wir $p^2 - 1 = 8(2m + 1)(m + 1)$.

Weitere Beweistechniken, wie die vollständige Induktion und kombinatorische Beweise werden später besprochen.