Théorie des nombres III

Thomas Huber

Actualisé: 19 avril 2016
vers. 1.6.8

Table des matières

1 Équations particulières

1.1 Équations quadratiques

Les équations quadratiques à coefficients entiers sont très importants en théorie des nombres. De manière cachée elles apparaissent beaucoup plus souvent que ce qu'on pourrait croire. Une équation quadratique en x a la forme

$$ax^2 + bx + c = 0,$$

où $a \neq 0, b, c$ sont des constantes réelles. Elle possède deux solutions (complexe) x_1, x_2, qui peuvent coïncider. On a

$$x_{1,2} = \frac{-b \pm \sqrt{D}}{2a},$$

où $D = b^2 - 4ac$ est le *discriminant* de l'équation. Ce nom est du au fait que le signe de D nous donne des informations sur l'ensemble des solutions :

$D > 0$	$\Leftrightarrow$	Deux solutions réelles distinctes.
$D = 0$	$\Leftrightarrow$	Une solution réelle double.
$D < 0$	$\Leftrightarrow$	Deux solutions complexes conjuguées.

Le cas important pour nous est le cas de coefficients entiers. Sous quelles hypothèse y-a-t-il des solutions entières ? Nécessaire (mais pas suffisant) est la condition que D est un carré. On peut souvent exploiter ce fait.

Exemple 1. *Trouver toutes les solutions entières positives de l'équation*

$$xyz = x^2 + y + z.$$

Solution. Malgré le fait que le côté gauche est de degré 3 on a ici une équation quadratique en x. Le discriminant vaut

$$D = y^2z^2 - 4(y + z).$$

Pour une solution entière D doit être un carré. Mais on a toujours $(yz)^2 > D$. Si de plus l'inéquation $4(y + z) < 2yz - 1$ est satisfaite D est entre les carrés consécutifs $(yz - 1)^2$ et $(yz)^2$ ne peut être un carré. Il suffit donc de considérer les paires (y, z) avec $4(y + z) \geq 2yz - 1$. Cette inéquation est équivalente à

$$(y - 2)(z - 2) \leq 4.$$

Donc y ou z doit être plus petit que 3 ou encore (y, z) est une des paires $(3, 3), (3, 4), (3, 5), (3, 6), (4, 4)$ ou une transposée. On laisse l'analyse de ces cas au lecteur. Les solutions (x, y, z) avec $y \geq z$ sont :

$$(2, 5, 1), (3, 5, 1), (2, 2, 2), (1, 3, 2), (5, 3, 2).$$

□

Si on essaye de trouver les cas où le discriminant est un carré on devrait travailler avec des estimations. Généralement cela est très efficace. Des manipulations algébriques et des calculs de modulo peuvent mener au but mais souvent il faut faire quelques détours.

Le théorème de Viète est encore plus important que le discriminant. Rappel : Si $x_{1,2}$ sont les deux solutions de $x^2 + px + q = 0$, alors on a

$$x_1 + x_2 = -p$$
$$x_1 \cdot x_2 = q$$

En particulier on peut conclure que si p, q sont entiers et si l'équation a une solution alors la deuxième solution est aussi entière. Ceci a une grande importance comme on va voir. Ça permet en fait de construire de nouvelles solutions à partir de solutions connues. D'un côté on peut montrer l'existence de solutions avec certaines propriétés d'un autre côté ceci aide à estimer. Des fois on s'intéresse pas à toutes les solutions mais on peut en choisir une. Dans ce cas il est souvent intéressant e choisir une solution *minimale* et d'aplliquer Viète. L'exemple par excellence est la solution magnifique d'un exercie d'OIM vraiment difficile.

Exemple 2 (OIM 88)**.** *Soient a, b des nombres naturels tels que $a^2 + b^2$ est divisible par $ab + 1$. Montrer que*

$$\frac{a^2 + b^2}{ab + 1}$$

est un carré.

Solution. Supposons

$$\frac{a^2 + b^2}{ab + 1} = q \tag{1}$$

avec un naturel q qui n'est pas un carré. Puisque (1) est symétrique en a et b on peut supposer $a \geq b$. Parmi toutes les paires (a, b) avec $a \geq b > 0$ vérifiant (1) on choisit celles avec a *minimale* et parmi celles là celle avec b *minimal*. On peut maintenant transforme (1) en une équation quadratique en a :

$$a^2 - a \cdot qb + (b^2 - q) = 0.$$

Elle a une autre solution a' et d'après Viète on a

$$a + a' = qb$$
$$a \cdot a' = b^2 - q.$$

De la première équation découle que a' est aussi entier. D'après la construction la paire (a', b) satisfait aussi (1) et donc $a' \geq 0$ (car sinon $a'b + 1 = 0$ ou $q < 0$). Avec la deuxième

équation one peut conclure que $a' > 0$ car sinon on aurati $q = b^2$ donc un carré. De plus on peut dire que $aa' = b^2 - q < b^2 \leq a^2$, donc $0 < a' < a$. Mais cela veut dire que la paire (a', b) ou la paire (b, a') contredit le chois minimal de (a, b), contradiction. Donc q doit être un carré. □

Exemple 3 (Taiwan 98)**.** *Existe-t-il une solution entière de l'équation*

$$x^2 + y^2 + z^2 + u^2 + v^2 = xyzuv - 65$$

avec les entiers x, y, z, u, v *plus grandes que* 1998 *?*

Soltuion. Le côté gauche est de degré 2, le côté droit est essentiellement de degré 5. Si toutes les variables sont grandes le côté gauche devrait être beaucoup plus grand que le côté gauche. mais au côté gauch il y a des carrés purs et à droite des termes mixtes. Alors si par exemple x est beaucoup plus grand que y, z, u, v les deux côté pourraient valoir la même chose. Il faut donc faire attention. Effectivement la réponse est oui.
On va montrer plus généralement que des solutions de cette équation existent et que la plus petite des cinq variables est arbitrairement grand.
Supposons qu'on ait une solution positive $(x_1, y_1, z_1, u_1, v_1)$ et que pas tous les cinq nombres sont égaux. Grâce à la symétrie on peut supposer $x_1 \leq \ldots \leq v_1$ et on a en particulier $x_1 < v_1$. On regarde l'équation comme équation quadratique en x C'est-à-dire x_1 est solution de

$$x^2 - (y_1 z_1 u_1 v_1)x + (y_1^2 + z_1^2 + u_1^2 + v_1^2 - 65) = 0$$

D'après Viète la deuxième solution $x_2 = y_1 z_1 u_1 v_1 - x_1$ est aussi entière. De plus Viète nous dit que $x_1 x_2 = y_1^2 + z_1^2 + u_1^2 + v_1^2 + 65 > v_1^2$ puisque $x_1 < v_1$ donc $x_2 > v_1$. On obtient alors une nouvelle solution $(y_1, z_1, u_1, v_1, x_2)$ où pas tous les nombres sont distincts. Au plus tard après 4 de ces opérations l'élémen t le plus petit a augmenté. En effectuant assez souvent cette opération on peut rendre tous les nombres arbitrairement grand, en particulier plus grand que 1998.
Il reste à trouver une solution. Une recherche excessive nous donne par exemple les solution $(1, 2, 3, 4, 5)$ et $(1, 1, 3, 8, 10)$. □

1.2 Triplets de Pythagore

Un triple (x, y, z) d'entiers positifs qui satisfait l'équation

$$x^2 + y^2 = z^2$$

s'appelle *triplet de Pythagore*. Si x, y et z ont un diviseur commun q alors on a aussi la solution $(\frac{x}{q}, \frac{y}{q}, \frac{z}{q})$ et on va supposer que ce ne soit pas le cas. Alors les trois nombres sont deux-à-deux premiers entre eux car un diviseur commun de deux divise aussi le troisième comme on peut remarquer facilement. Un tel triple est appelé *primitif*. Dans un triple primitif au plus un nombre peut être pair. D'autre part pas tous les trois peuvent être

impairs, sinon le côté gauche serait pair et le côté droit impair.
De plus z ne peut être pair car sinon le côté gauche serait $\equiv 2$, et le côté droit $\equiv 0 \pmod 4$. Le théorème ci-dessous explique la structure des triplets de Pythagore.

Théorème 1.1. *Les conditions suivantes sont équivalentes :*

(a) $x^2 + y^2 = z^2$, *avec des naturels* x, y, z *et* y *premiers entre eux et* y *pair.*

(b) Il existe des nombres positifs m *et* n *premiers entre eux avec* $m > n, m \not\equiv n \pmod 2$ *et*

$$x = m^2 - n^2, \quad y = 2mn, \quad z = m^2 + n^2.$$

Preuve. Supposon (x, y, z) soient comme dans (a). Alors on a $y^2 = (z-x)(z+x)$ et donc $y = 2v, z + x = 2u$ et $z - x = 2w$ sont pairs. Puisque x et z sont premiers entre eux, on a la même propriété pour u et w. On remplace pour remarquer que les deux sont des carrés. $u = m^2$, $w = n^2$. De plus u et w ne sont pas les deux pairs et donc $m \not\equiv n \pmod 2$. Exprimant x, y, z par m et n on obtient (b). Inversement un triple (x, y, z) comme dans (b) satisfait aussi (a). □

Il y a donc un nombre infini de triplets de Pythagore primitifs. C'est bien connu que le résultat devient faux si l'exponent est supérieur à 2. Pour la complétude on va citer le résultat même si la preuve est légèrement au dessus du niveau de ce skript :

Théorème 1.2 (Le dernier théorème de Fermat)**.** *Pour* $n > 3$ $(1, 0, 1)$ *et* $(0, 1, 1)$ *sont les seules solutions sans diviseurs communs en entiers positifs de l'équation*

$$x^n + y^n = z^n.$$

Au moins on peut facilement remarquer la chose suivante : il suffit de prouver le théorPme pour n premier et $n = 4$. Le premier cas est très difficile et a été prouvé en 1995 par A. Wiles. Le cas $n = 4$ est élémmentaire et laissé en exercices.

1.3 Die Pell Gleichung

Bei der *Pell Gleichung* handelt es sich um eine quadratische Gleichung in zwei Variablen, die in vielen Problemen ganz natürlich auftaucht. In ihrer einfachsten Form lautet sie

$$x^2 - Dy^2 = 1 \tag{2}$$

wobei $D > 1$ eine natürliche Zahl ist, die durch kein Quadrat > 1 teilbar ist (man nennt D *quadratfrei*). Dies kann man übrigens immer annehmen, denn wenn D einen quadratischen Faktor hat, kann man diesen durch eine Umdefinition von y entfernen.
Um alle positiven, ganzen Lösungen dieser Gleichung zu finden, geht man in zwei Schritten vor :

— Finde die kleinste positive Lösung.

— Konstruiere daraus rekursiv alle anderen.

Zentral für das Folgende ist die Faktorisierung

$$x^2 - Dy^2 = (x + \sqrt{D}y)(x - \sqrt{D}y). \tag{3}$$

Wir assoziieren zu jeder positiven Lösung (x, y) die Zahl $a = x + \sqrt{D}y$. Beachte, dass sich (x, y) aus a rekonstruieren lässt, denn aus $x + \sqrt{D}y = u + \sqrt{D}v$ folgt $x = u$ und $y = z$, da D quadratfrei ist. Aus (3) folgt ausserdem : ist (x, y) eine Lösung von (2), dann gilt $x + \sqrt{D}y > 1$ und $0 < x - \sqrt{D}y < 1$.
Zuerst zur Minimalen Lösung. Eine positive Lösung (x_0, y_0) heisst *minimal*, falls $x_0 + \sqrt{D}y_0$ minimal ist unter allen positiven Lösungen. Sind (x_1, y_1) und (x_2, y_2) zwei positive Lösungen von (2), dann gilt $x_1 < x_2$ genau dann, wenn $y_1 < y_2$. Wenn es also überhaupt eine positive Lösung gibt, dann auch eine eindeutig bestimmte kleinste (x_0, y_0). Man kann beweisen, dass die Gleichung (2) *immer* eine positive Lösung besitzt, dies ist aber nicht einfach. Im konkreten Anwendungsfall findet man die minimale Lösung meist schnell durch probieren. Sie kann in manchen Fällen aber auch erschreckend gross sein. Es gibt ein allgemeines Verfahren, wie man (x_0, y_0) berechnen kann. Dazu muss man die minimalen Perioden in der Kettenbruchentwicklung von D bestimmen. Dies zu erklären, würde aber den Rahmen hier sprengen.

Nun wenden wir uns der Konstruktion *aller* Lösungen zu.

Théorème 1.3. *Nehme an,* (x_0, y_0) *sei die minimale positive Lösung von* (2). *Definiere rekursiv die Folgen*

$$x_{n+1} = x_0 x_n + D y_0 y_n$$
$$y_{n+1} = y_0 x_n + x_0 y_n.$$

Die positiven Lösungen von (2) *sind dann genau die Paare* (x_n, y_n) *für* $n \geq 0$. *Insbesondere gibt es beliebig grosse Lösungen.*

Beweis. Mit vollständiger Induktion zeigt man leicht, dass x_n, y_n gerade so konstruiert sind, dass gilt

$$x_n + \sqrt{D}y_n = (x_0 + \sqrt{D}y_0)^{n+1}.$$

Aus (3) folgt, dass wenn $u + \sqrt{D}v$ und $w + \sqrt{D}z$ Lösungen sind, dann auch ihr Produkt und ihr Quotient. Mit obiger Formel folgt daraus, dass alle (x_n, y_n) Lösungen sind. Nehme nun an, es existiert eine weitere Lösung $u + \sqrt{D}v$, die nicht von dieser Form ist. Dann gibt es ein n mit

$$(x_0 + \sqrt{D}y_0)^n < u + \sqrt{D}v < (x_0 + \sqrt{D}y_0)^{n+1}.$$

Multiplikation mit $(x_0 - Dy_0)^n$ liefert

$$1 < (u + \sqrt{D}v)(x_0 - \sqrt{D}y_0)^n < x_0 + \sqrt{D}y_0$$

Der mittlere Term ist grösser als 1 und daher eine positive Lösung von (2). Die rechte Ungleichung widerspricht aber der Minimalität von (x_0, y_0). □

Exemple 4. *Zeige, dass es unendlich viele Dreiecke gibt, sodass die Seitenlängen drei aufeinanderfolgende ganze Zahlen sind und auch der Flächeninhalt ganz ist.*

Lösung. Seien $a = n-1, b = n$ und $c = n+1$ die Seitenlängen des Dreiecks. Nach Heron ist die Fläche gegeben durch

$$A = \frac{1}{4}\sqrt{(a+b+c)(a+b-c)(a-b+c)(-a+b+c)} = \frac{n}{4}\sqrt{3(n^2-4)}$$

Damit A eine ganze Zahl ist, muss n gerade sein und der Ausdruck unter der Klammer eine Quadratzahl. Ersetze n durch $2x$ und $\frac{A}{n}$ durch m, dann wird die Gleichung zu $3x^2 - 3 = m^2$. Daraus folgt, dass m durch 3 teilbar ist, setze also $m = 3y$. Die Gleichung wird zu

$$x^2 - 3y^2 = 1.$$

Dies ist eine Pell Gleichung mit minimaler Lösung $(x_0, y_0) = (2, 1)$. Die anderen Lösungen sind gegeben durch die Rekursionen $x_{n+1} = 2x_n + 3y_n$ und $y_{n+1} = x_n + 2y_n$. Die ersten Lösungen lauten

$$(2,1), (7,4), (26,15), (97,56), (362,209), \ldots$$

Die gesuchten Dreiecke sind also genau die mit den Seitenlängen $2x_n - 1, 2x_n, 2x_n + 1$ und haben die Fläche $3x_n y_n$. Insbesondere gibt es unendlich viele davon. □

Die *verallgemeinerte Pell Gleichung* hat die Form

$$ax^2 - by^2 = c \tag{4}$$

mit ganzen Zahlen a, b, c, wobei a und b positiv und quadratfrei sind, und nicht beide gleich 1. Wenn a und b beide grösser als 1 sind, kann es mehrere kleinste Lösungen, sogenannte Fundamentallösungen, geben. Die ganze Geschichte wird dann sehr kompliziert. Wir beschränken uns daher auf den Fall, wo $a = 1$ oder $b = 1$ ist. Den Fall $a = c = 1$ haben wir oben ausführlich diskutiert. Wir geben nun eine Übersicht über die weiteren Resultate. Die Beweise sind nicht schwierig und dem Leser als Übung überlassen.

1. $b = c = 1$
   Die Gleichung hat dann die Form $ax^2 - y^2 = 1$ und lässt sich umschreiben zu $y^2 - ax^2 = -1$. Dieser Fall lässt sich daher auf den nächsten zurückführen.
2. $a = 1$
   Die Gleichung hat die Form
   $$x^2 - by^2 = c.$$
   Falls die Gleichung $x^2 - by^2 = c$ eine positive Lösung hat, gibt es unendlich viele solche. Sei (x_0, y_0) die kleinste und (x_1, y_1) die zweitkleinste Lösung. Definiere (p, q) durch
   $$\frac{x_1 + \sqrt{b}y_1}{x_0 + \sqrt{b}y_0} = p + \sqrt{b}q.$$

p und q sind wohldefinierte positive rationale Zahlen (nach Konstruktion ist (p, q) eine rationale Lösung der Gleichung $x^2 - by^2 = 1$, die im Allgemeinen kleiner ist, als die minimale ganzzahlige positive Lösung).
Die Gesamtheit der positiven Lösungen ist dann gegeben durch

$$x_n + \sqrt{b}y_n = (p + \sqrt{b}q)^n(x_0 + \sqrt{b}y_0), n \geq 0.$$

Mit anderen Worten, die Lösungen (x_n, y_n) erhält man über die Rekursionsgleichungen

$$x_{n+1} = px_n + bqy_n,$$
$$y_{n+1} = qx_n + py_n.$$

Wenn $c \neq 1$, kann es auch sein, dass die Gleichung gar keine Lösungen besitzt, im Gegensatz zum Fall $c = 1$. Dies lässt sich oft mit Hilfe der Modulorechnung beweisen.

Exemple 5. *Zeige, dass die Gleichung $x^2 - 7y^2 = -1$ keine ganzzahlige Lösung besitzt.*

Lösung. Betrachte die Gleichung modulo 7. Dann muss gelten $x^2 \equiv 6 \pmod 7$. Dies ist nicht möglich. □

Exemple 6 (Shortlist 95)**.** *Finde die kleinste natürliche Zahl n, sodass $19n + 1$ und $95n + 1$ beides Quadrate sind.*

Lösung. Setze $95n + 1 = x^2$ und $19n + 1 = y^2$. Dann muss gelten $x^2 - 5y^2 = -4$. Dies ist eine verallgemeinerte Pell Gleichung. Die beiden kleinsten Lösungen sind $(1, 1)$ und $(4, 2)$, daraus berechnet man leicht $(p, q) = (\frac{3}{2}, \frac{1}{2})$. Mit Hilfe der Rekursionsformeln

$$x_{n+1} = \frac{3x_n}{2} + \frac{5y_n}{2}$$
$$y_{n+1} = \frac{3y_n}{2} + \frac{x_n}{2}$$

Findet man die ersten paar Werte von y_n :

$$1, 2, 5, 13, 34, 89, 233, 610, 1597, \ldots$$

Der Wert $y_0 = 1$ führt zu $n = 0$, ist also nicht zu beachten. Wegen $y^2 = 19n + 1$ suchen wir also die erste Zahl in dieser Lösungsfolge, deren Quadrat $\equiv 1 \pmod{19}$ ist. Eine kurze Rechnung zeigt, dass dies $y_8 = 1597$ ist. Die Antwort lautet daher :

$$n = \frac{1}{19}(y_8^2 - 1) = 134232.$$

□

1.4 Construction de solutions

Dans cette section on essaye de montrer quelques méthodes qui servent à la construction de solutions de problèmes en théorie des nombres. Souvent on n'exige pas de trouver *toutes* les solutions mais seulement quelques-unes (où une infinité).
Il y a beaucoup de techniques différentes et on va les montrer avec des exemples.

Exemple 7 (Canada 91)**.** *Montrer que l'équation*

$$x^2 + y^5 = z^3$$

admet une infinité de solutions entières avec $xyz \neq 0$.

Solution. La solution $(x, y, z) = (3, -1, 2)$ satisfait $xyz \neq 0$. L'équation est dans un certain sens homogène, autrement dit chaque variable y est qu'avec un seul exposant et il n'y a pas de terme constant. Donc si (x, y, z) est une solution avec $xyz \neq 0$ alors on a aussi la solution $(a^{15}x, a^6y, a^{10}z)$ pour tout $a = 0$. En particulier il y a une infinité de solution. □

Dans cet exemple en multipliant la solution par certains facteurs. Mais ce n'est pas toujours possible. L'exemple suivant est trop inhomogène pour ça ;

Exemple 8 (Italie 96)**.** *Montrer que l'équation*

$$a^2 + b^2 = c^2 + 3$$

admet une infinité de solutions entières.

Solution. Si a est un entier impair alors on pose $b = \frac{a^2-5}{2}$ et $c = \frac{a^2-1}{2}$. Maintenant on a

$$c^2 - b^2 = (c + b)(c - b) = a^2 - 3.$$

□

Ici on a pu trouver explicitement toute une famille de solutions. On s'est fait inspirer pour les expression de b et c par les formules binomiales. Souvent construire des carrés, bricoler avec des carrés, cubes etc. est une approche prometteuse. Encore un exemple :

Exemple 9. *Montrer que pour tout naturel* m *il existe un naturel* n *tel que* $m + n + 1$ *est un carré et* $mn + 1$ *un cube*

Solution. $m(m^2 + 3m + 3) + 1 = (m + 1)^3$ est par exemple un cube de la forme $mn + 1$. Et effectivement dans ce cas on a m+n+$1 = m^2 + 4m + 4 = (m + 2)^2$ .On peut donc simplement poser $n = m^2 + 3m + 3$. □

Une méthode très important est la construction par récurrence. L'idée est simple. Si on a une solution du problème on peut construire une autre (plus grande, meilleure etc.) avec.

Exemple 10 (OIM 89)**.** *Montrer : pour tout naturel n il existe n naturels consécutifs dont aucun est une puissance d'un premier.*

Solution. On fait une récurrence par n. Pour $n = 1$ on peut choisir 6. Soit $k > 1$ et soient

$$k - n, k - n + 1, \ldots, k - 1$$

n naturels consécutifs dont aucun n'est une puissance d'un premier. Alors

$$k \cdot k! + (k - n), k \cdot k! + (k - n + 1), \ldots, k \cdot k! + (k - 1), k \cdot k! + k$$

sont $n+1$ nombres consécutifs dont aucun n'est puissance d'un premier. Car $k \cdot k! + (k - i)$ est divisible par $k - i$ pour $i = 1, \ldots, n$. Mais par hypothèse de récurrence $k - i$ n'est pas puissance d'un premier donc $k \cdot k! + (k - i)$ non plus. D'ailleurs $k \cdot k! + k = k(k! + 1)$ est un produit de deux naturels premiers entre eux > 1, donc pas puissance d'un premier. Ceci complète le pas de récurrence. □

Exemple 11 (OIM 71)**.** *Montrer qu'il existe une infinité de nombres de la forme $2n - 3$ qui sont deux-à-deux premiers entre eux.*

Solution. Il suffit de montre la chose suivante : Si $n_1, \ldots, n_k$ sont différents et $2^{n_1} - 3, \ldots, 2^{n_k} - 3$ deux-à-deux premiers entre eux, alors il existe un n_{k+1}, tel que $2^{n_{k+1}} - 3$ n'a pas de diviseur commun avec les nombres déjà construits.
Soit $\{p_1, \ldots, p_r\}$ l'ensemble des premiers qui divisent un des nombres $2^{n_1} - 3, \ldots, 2^{n_k} - 3$. Posons $n_{k+1} = (p1 - 1)(p2 - 1) \ldots (pr - 1) + 1$. Maintenant on a pour tout $i = 1, \ldots, r$

$$2^{n_{k+1}} - 3 = 2 \cdot 2^{(p_1 - 1) \ldots (p_r - 1)} - 3 \equiv 1 \pmod{p_i}$$

puisque d'après le petit théorème de Fermat on a $2^{p_i - 1} \equiv 1 \pmod{p_i}$. Donc $2^{n_{k+1}} - 3$ n'est pa divisible par p_i, ce qui signifie par construction des p_i que ce nombre n'a pas de diviseur commun avec $2n_1 - 3, \ldots, 2^{n_k} - 3$. Ceci termine la preuve. □

On peut aussi utiliser le théorème des restes chinois pour construire des solutions, voir l'exemple **??**. Une autre possibilité a été présenté dans le paragraphe précédent : les équations de Pell. Si on peut réduire l'existence de solutions à une équation de Pell, alors il suffit de trouver une seule solution de cette équation pour conclure qu'il y en a une infinité. Voir les exemples 4 et 6. On doit aussi penser au rapport entre les deux solutions d'une équation quadratique. On peut des fois passer d'une solution d'une équation quadratique. On peut des fois passer d'une solution à l'autre. Et une remarque finale : Dans certaines cas rares on peut prouver par l'absurde qu'il existe une infinité de chose avec une certaine propriété, comme par exemple dans le script de Théorie des nombres I dans la preuve de l'existence d'une infinité de nombres premiers

2 Kongruenzen II

2.1 Ordnungen

Sei n eine natürliche Zahl. Wir haben den Begriff der Ordnung einer Zahl modulo n bereits in Zahlentheorie II eingeführt. Hier nochmals die Definition : Ist a teilerfremd zu n, dann gibt es eine kleinste positive ganze Zahl d, sodass $a^d \equiv 1 \pmod{n}$ gilt. Dieses d heisst die Ordnung von a modulo n. Dass es überhaupt einen Exponenten $e > 0$ gibt mit $a^e \equiv 1 \pmod{n}$ folgt zum Beispiel aus dem Satz von Euler-Fermat, man kann nämlich $e = \varphi(n)$ wählen. Im Allgemeinen ist d aber viel kleiner als $\varphi(n)$ und schwierig zu berechnen. Wichtig ist die Ordnung vor allem wegen folgender Tatsache :

Lemme 2.1. *Sei a teilerfremd zu n und sei d die Ordnung von $a \pmod{n}$. Für eine ganze Zahl m gilt genau dann $a^m \equiv 1 \pmod{n}$, wenn m durch d teilbar ist.*

Beweis. Schreibe $m = kd + r$ mit ganzen Zahlen k, r und $0 \leq r < d$ (Division mit Rest). Nun gilt nach den Potenzgesetzen

$$a^m = a^{kd+r} = (a^d)^k \cdot a^r \equiv 1^k \cdot a^r = a^r \pmod{n},$$

also gilt $a^m \equiv 1$ genau dann, wenn auch $a^r \equiv 1$ ist. Nun ist aber $r < d$ und per Definition ist d ja die *kleinste* natürliche Zahl mit $a^d \equiv 1$. Daher gilt $a^r \equiv 1$ nur für $r = 0$, also genau dann wenn m durch d teilbar ist. □

Insbesondere ist also d immer ein Teiler von $\varphi(m)$. In manchen Situationen kann man nun zeigen, dass d auch ein Teiler einer anderen Zahl sein muss, die beinahe teilerfremd zu $\varphi(m)$ ist. Als Konsequenz ist dann d sehr klein, und genau das kann man oft brauchen. Als klassisches Beispiel besprechen wir den ersten Teil der Lösung einer alten IMO-Aufgabe.

Exemple 12 (IMO 90)**.** *Finde alle natürlichen Zahlen n, sodass*

$$\frac{2^n + 1}{n^2}$$

eine ganze Zahl ist.

Lösung. Offenbar ist $n = 1$ eine Lösung. Wir nehmen nun $n > 1$ an und zeigen, dass der kleinste Primteiler von n gleich 3 sein muss. Offenbar ist n ungerade. Sei also p dieser kleinste Primteiler und sei d die Ordnung von 2 modulo p. Nach Voraussetzung ist jetzt p ein Teiler von $2^n + 1$, also gilt $2^n \equiv -1$ und quadrieren liefert $2^{2n} \equiv 1 \pmod{p}$. Mit Lemma 2.1 können wir diese Kongruenzen nun in Teilbarkeitsaussagen für d umschreiben :

$$2^n \not\equiv 1 \pmod{p} \Longrightarrow d \nmid n, \qquad 2^{2n} \equiv 1 \pmod{p} \Longrightarrow d \mid 2n.$$

Ausserdem gilt sowieso $d \mid \varphi(p) = p - 1$. In Kombination muss d also sogar $\mathrm{ggT}(2n, p-1)$ teilen ! An dieser Stelle kommt nun ins Spiel, dass wir p als minimalen Primteiler von

n gewählt haben. Dies impliziert nämlich, dass $p-1$ nur Primteiler besitzt, die n nicht teilen. Also sind n und $p-1$ teilerfremd und somit gilt $\mathrm{ggT}(2n, p-1) = 2$. Das bedeutet $d = 1$ oder $d = 2$, der erste Fall kann aber nicht eintreten, denn sonst wäre d ein Teiler von n, was noch obigen Rechnungen nicht sein kann. Jetzt gilt also nach Definition der Ordnung $2^2 \equiv 1 \pmod{p}$ und das kann nur für $p = 3$ gelten. □

Der entscheidende Punkt in diese Argument war, dass d sowohl $2n$ als auch $p-1$ teilen muss, und dass diese beiden Zahlen wirklich beinahe teilerfremd sind. Das Ganze hat deswegen funktioniert, weil p sowohl ein Teiler des Ausdrucks $2n+1$ vorkommt, also auch im Exponenten von 2 auftaucht (als Teiler von n). Das ist genau die Situation, wo man zwei grundsätzlich verschiede Teilbarkeitsbedingungen für d kriegt. Die Idee, den kleinsten Primteiler einer Zahl mit solchen Methoden zu bestimmen, ist ganz wichtig und führt oft zum Ziel.

Die obige Lösung kann man wie folgt beenden : Zuerst zeigt man, dass n nicht durch 9 teilbar ist. Das ist der schwierigste Schritt. Danach hat man also $n = 3m$, wo m nicht durch 3 teilbar ist. Der letzte Schritt besteht dann darin zu zeigen, dass der kleinste Primteiler von m gleich 7 ist, was dann schnell auf einen Widerspruch führt. Dieser Schritt ist beinahe identisch zum obigen Argument und euch als Übung empfohlen.

Eine weitere wichtige Anwendung ist folgendes schönes Resultat, das doch recht überraschend ist :

Exemple 13. *Sei p eine ungerade Primzahl und seien a, b zwei ganze Zahlen, die nicht durch p teilbar sind. Ist dann $a^{2^n} + b^{2^n}$ durch p teilbar, dann gilt $p \equiv 1 \pmod{2^{n+1}}$.*

Lösung. Sei b^{-1} ein multiplikatives Inverses von b modulo p, also eine ganze Zahl mit $b \cdot b^{-1} \equiv 1 \pmod{p}$. Zum Beispiel kann man $b^{-1} = b^{p-2}$ wählen nach dem kleinen Satz von Fermat (nach Voraussetzung ist ja b nicht durch p teilbar). Nun gilt

$$a^{2^n} + b^{2^n} \equiv 0 \Longleftrightarrow a^{2^n} \equiv -b^{2^n} \Longleftrightarrow (ab^{-1})^{2^n} \equiv -1 \pmod{p}.$$

Sei d die Ordnung von ab^{-1} modulo p. Dann folgt aus der Kongruenz oben ähnlich wie im letzten Beispiel, dass d kein Teiler von 2^n aber ein Teiler von 2^{n+1} ist (für ersteres braucht man, dass $p \neq 2$ ist, denn sonst gilt $-1 \equiv 1$). Das kann aber nur für $d = 2^{n+1}$ der Fall sein. Ausserdem teilt d wie immer $\varphi(p) = p-1$, also gilt $p \equiv 1 \pmod{2^{n+1}}$ wie gewünscht. □

Die Aussage sieht doch recht technisch aus, wir schlachten sie daher noch ein bisschen aus. Es folgt nämlich zum Beispiel :

- Sind a und b teilerfremd, dann ist jeder ungerade Primteiler von $a^{2^n} + b^{2^n}$ kongruent zu $1 \pmod{2^{n+1}}$! Das gilt insbesondere im wichtigen Spezialfall $b = 1$.
- Noch spezieller ist der Fall $a = 2, b = 1$. Man erhält die sogenannten Fermat Zahlen $F_n = 2^{2^n} + 1$, von denen Fermat fälschlicherweise vermutete, dass sie alle prim sind. Zum Beispiel besitzt F_5 den Primteiler 641. Trotzdem sind die Primteiler von F_n

recht gross, denn sie sind alle $\equiv 1 \pmod{2^{n+1}}$, also sicher nicht kleiner als $2^{n+1}+1$. Dies ist der Grund, wieso die Fermat Zahlen sehr schwierig zu faktorisieren sind.

— Ist $p \equiv 3 \pmod 4$ ein Primteiler von a^2+b^2 , dann teilt p sogar a und b.

— Wir haben früher schon gesehen, dass die Pell-Gleichung $x^2 - Dy^2 = -1$ nicht immer eine Lösung besitzt. Wir können jetzt eine starke Bedingung an D ableiten, die erfüllt sein muss, wenn die Gleichung Lösungen besitzt. Umformen liefert nämlich $Dy^2 = x^2 + 1$, daher teilt jeder Primteiler von D die rechte Seite. Also ist jeder ungerade Primteiler von D (und auch von y) $\equiv 1 \pmod 4$.

In allen bisherigen Beispielen konnten wir durch betrachten von Ordnungen Aussagen über die Primteiler verschiedener Zahlen machen. Das ist ganz allgemein das Ziel der Sache. Keine andere Methode, die wir kennengelernt haben, liefert ähnlich starke Aussagen. Daher sind Ordnungen auch ein unverzichtbares technischen Hilfsmittel bei der Lösung von zahlentheoretischen Problemen.

Als letztes Beispiel noch ein bekanntes und nützliches Resultat über die Primteiler von geometrischen Folgen. Wir erinnern daran, dass für $a \neq 1$ und jede natürliche Zahl n die Formel $a^{n-1} + a^{n-2} + \ldots + a + 1 = \frac{a^n-1}{a-1}$ gilt.

Exemple 14. *Sei p eine Primzahl und $a \neq 1$ eine ganze Zahl. Ist q ein Primteiler von*

$$\frac{a^p - 1}{a - 1}$$

dann gilt $q = p$ oder $q \equiv 1 \pmod p$. Dann kann der Fall $p = q$ nur dann auftreten, wenn $p \,|\, a - 1$.

Lösung. Sei q ein solcher Primteiler und sei d die Ordnung von a modulo q. Dann gilt $q \,|\, a^p - 1$, also $a^p \equiv 1 \pmod q$. Daraus folgt $d \,|\, p$ und da p prim ist also $d = 1$ oder $d = p$. Wir analysieren zuerst den ersten Fall $d = 1$. Dann ist q auch ein Teiler des Nenners $a - 1$, wir berechnen daher den ggT von Zähler und Nenner :

$$\begin{aligned}(a^p - 1, a - 1) &= (a^{p-1} + a^{p-2} + ... + a + 1, a - 1) = (2a^{p-2} + a^{p-3} + ... + a + 1, a - 1) \\ &= (3a^{p-3} + a^{p-4} + ... + a + 1, a - 1) = ... = (pa, a - 1) = (p, a - 1),\end{aligned}$$

denn $a - 1$ ist teilerfremd zu a. Also muss q ein Teiler von p, also gleich p sein. Dies gilt genau dann, wenn $p \,|\, a - 1$. Im Fall $d = p$ folgt $p = d \,|\, \varphi(q) = q - 1$, also $q \equiv 1 \pmod p$. □

2.2 Primitive Wurzeln

Sei n eine natürliche Zahl und a teilerfremd zu n. Wir haben gesehen, dass die Ordnung von a modulo n immer ein Teiler von $\varphi(n)$ ist. Wir nennen a eine primitive Wurzel modulo n, falls a die maximal mögliche Ordnung $\varphi(n)$ besitzt. Zum Beispiel rechnet man leicht nach, dass 9 eine primitive Wurzel modulo 17 ist, dass 11 eine primitive Wurzel modulo

18 und dass 2 eine primitive Wurzel modulo 19 ist. Im Gegensatz dazu existiert keine primitive Wurzel modulo 20, denn trotz $\varphi(20) = 8$ gilt stets $a^4 \equiv 1$ wenn a teilerfremd zu 20 ist.

Existiert eine primitive Wurzel a modulo n, dann sind die Potenzen $1, a, a^2, \dots a^{\varphi(n)-1}$ paarweise nicht kongruent mod(n) und durchlaufen daher die zu n teilerfremden Restklassen genau einmal. Somit lässt sich das Rechnen mit dieses Restklassen auf das Rechnen mit Potenzen von a zurückführen, was natürlich wesentlich einfacher ist.

Entscheidend für diesen Abschnitt ist nun das folgende Resultat, das wir mit unseren Mitteln leider nicht beweisen können :

Théorème 2.2. *Jede Primzahl besitzt eine primitive Wurzel.*

Bevor wir uns der allgemeinen Situation zuwenden, zuerst ein Beispiel für die Nützlichkeit von primitiven Wurzeln.

Exemple 15 (SMO 03)**.** *Finde die grösste natürliche Zahl n, die für alle ganzen Zahlen a ein Teiler von $a^{25} - a$ ist.*

Lösung. Zuerst zeigen wir, dass n quadratfrei ist. Für jeden Primteiler p von n muss nämlich n nach Voraussetzung ein Teiler von $p^{25} - p = p(p^{24} - 1)$ sein. Dann ist n aber sicher nicht durch p^2 teilbar.
Sei nun p ein Primteiler von n. Sei a eine ganze Zahl, die nicht durch p teilbar ist, und sei d die Ordnung von a modulo p. Wegen $a^{24} \equiv 1 \pmod{p}$ gilt $d \,|\, 24$ und allgemein haben wir $d \,|\, \varphi(p) = p - 1$. Wenn d sehr klein ist, gibt dies kaum Informationen über p. Interessant wird die Sache erst, wenn wir d im Verhältnis zu $p - 1$ sehr gross wählen können. Aber genau dies ist der Fall, wenn wir für a eine primitive Wurzel modulo p wählen, dann gilt ja sogar $d = p - 1$ und wir erhalten $p - 1 \,|\, 24$. Die einzigen Möglichkeiten sind demnach $p = 2, 3, 5, 7, 13$.
Umgekehrt folgt aus dem kleinen Satz von Fermat sofort, dass diese Primzahlen stets Teiler von $a^{25} - a$ sind, wir erhalten also die Lösung $n = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 = 2730$. □

Wir stellen nun das Hauptresultat dieses Abschnittes vor, dessen Beweis wir für den interessierten Leser ans Ende des Abschnittes verschieben.

Théorème 2.3.

(a) Es existiert genau in den folgenden Fällen eine primitive Wurzel modulo n :

- *(i)* $n = 2, 4$
- *(ii)* $n = p^k$ *für eine Primzahl* $p \geq 3$
- *(iii)* $n = 2p^k$ *für eine Primzahl* $p \geq 3$.

(b) Ist p prim und a eine primtive Wurzel modulo p, dann sind unter den Zahlen $a, a + p, \dots, a + (p - 1)p$ alle ausser genau einer primitive Wurzeln modulo p^2 .

(c) Ist $p \geq 3$ prim und ist a eine primitive Wurzel modulo p^2 , dann ist a auch eine primitive Wurzel modulo p^k für alle natürlichen Zahlen k.

(d) Für $k \geq 3$ hat 5 die Ordnung 2^{k-2} modulo 2^k und es gibt kein Element grösserer Ordnung. Jede ungerade Restklasse (mod $2k$) *lässt sich eindeutig in der Form $\pm 5^m$ mit $0 \leq m < 2^{k-1}$ schreiben.*

Am meisten mag vielleicht (c) erstaunen : Beispielsweise folgt daraus, dass 2 eine primitive Wurzel modulo allen 3er-Potenzen ist, denn 2 ist eine solche modulo 9. Diese Tatsache erlaubt es uns jetzt, die Lösung von Beispiel 12 sehr einfach zu vervollständigen

Lösung. Wir haben bereits gezeigt, dass $n = 1, 3$ Lösungen sind, und dass jede Lösung $n > 3$ durch 9 teilbar sein muss. Wir schreiben daher $n = 3^k m$ mit $k \geq 1$ und $3 \nmid m$. Nach Voraussetzung gilt $2^n \equiv -1 \pmod{3^{2k}}$ und da 2 eine primitive Wurzel modulo 3^{2k} ist, folgt für den Exponenten $n \equiv 3^{2k-1} \pmod{2 \cdot 3^{2k-1}}$. Das bedeutet aber, dass n durch 3^{2k-1} teilbar sein muss. Nach Definition von k ist somit $2k - 1 \leq k$, also $k = 1$. Dies zeigt, dass keine Lösungen $n > 3$ existieren. □

Der Rest dieses Abschnittes ist dem Beweis von Satz 2.3 gewidmet.
Die folgenden drei technischen Lemmata sind der Schlüssel zu allem. Wir bezeichnen die Ordnung von a modulo n abkürzend mit $\mathrm{ord}_n(a)$.

Lemme 2.4.

(a) Ist n eine natürliche Zahl und ist a teilerfremd zu n, dann gilt

$$\mathrm{ord}_n(a^k) = \frac{\mathrm{ord}_n(a)}{\mathrm{pgdc}(\mathrm{ord}_n(a), k))}.$$

(b) Sind $n_1, \ldots, n_k$ paarweise teilerfremde natürliche Zahlen und ist a teilerfremd zu $n_1 \ldots n_k$, dann gilt

$$\mathrm{ord}_{n_1 \cdots n_k}(a) = kgV(\mathrm{ord}_{n_1}(a), \ldots, \mathrm{ord}_{n_k}(a)).$$

(c) Ist $n_1 \mid n_2$ und a teilerfremd zu n_2 , dann gilt

$$\mathrm{ord}_{n_1}(a) \mid \mathrm{ord}_{n_2}(a) \quad \textit{und} \quad \frac{\mathrm{ord}_{n_2}(a)}{\mathrm{ord}_{n_1}(a)} \mid \frac{\varphi(n_2)}{\varphi(n_1)}$$

Beweis.

(a) Es gilt $(a^k)^m \equiv 1$ genau dann, wenn $\mathrm{ord}_n(a) \mid km$. Die kleinste natürliche Zahl m mit dieser Eigenschaft ist aber $m = \frac{\mathrm{ord}_n(a)}{ggT(\mathrm{ord}_n(a),k)}$.

(b) Es gilt $a^m \equiv 1 \pmod{n_1 \ldots n_k}$ genau dann, wenn $a^m \equiv 1 \pmod{n_i}$ gilt für $1 \leq i \leq k$. Letzteres ist genau dann der Fall, wenn m durch $\mathrm{ord}_{n_1}(a), \ldots, \mathrm{ord}_{n_k}(a)$ teilbar ist und die kleinste natürliche Zahl mit dieser Eigenschaft ist $m = kgV(\mathrm{ord}_{n_1}(a), \ldots, \mathrm{ord}_{n_k}(a))$.

(c) Ist $a^m \equiv 1 \pmod{n_2}$, dann natürlich auch $a^m \equiv 1 \pmod{n_1}$, dies zeigt $\mathrm{ord}_{n_1}(a) \mid \mathrm{ord}_{n_2}(a)$. Für den zweiten Teil können wir uns induktiv auf den Fall beschränken, wo $\frac{n_2}{n_1} = p$ eine Primzahl ist. Gilt $a^m \equiv 1 \pmod{n_1}$, dann ist $a = 1 + bn_1$ mit einer ganzen Zahl b. Wir betrachten nun zwei Fälle :

(i) Wenn n_1 durch p teilbar ist, dann gilt $\frac{\varphi(n_2)}{\varphi(n_1)} = p$. Nun ist

$$a^{mp} = (1 + bn_1)^p = 1 + bpn_1 + \sum_{i=2}^{p} \binom{p}{i} b^i n_1^i \equiv 1 \pmod{n_2},$$

denn alle Summanden ausser dem ersten sind durch n_2 teilbar (beachte : $n_2 \mid n_1^2$). Dies zeigt $\operatorname{ord}_{n_2}(a) \mid p \operatorname{ord}_{n_1}(a)$.

(ii) Wenn n_1 nicht durch p teilbar ist, dann gilt $\frac{\varphi(n_2}{\varphi(n_1)} = p - 1$. Da a nach Voraussetzung nicht durch p teilbar ist, gilt sicher $a^{p-1} \equiv 1 \pmod{p}$ und somit ist $a^{m(p-1)} \equiv 1 \pmod{n_2}$, also wieder $\operatorname{ord}_{n_2}(a) \mid (p-1) \operatorname{ord}_{n_1}(a)$.

□

Lemme 2.5. *Sei p eine Primzahl, $1 \leq b \leq p-1$ eine natürliche Zahl und sei a eine primitive Wurzel modulo p. Dann ist a oder $a + bp$ eine primitive Wurzel modulo p^2.*

Beweis. Nach Voraussetzung und Lemma 2.4 (c) haben a und $a + bp$ die Ordnung $p - 1$ oder $p(p-1) modulo p^2$. Wir nehmen nun an, beide Zahlen hätten die Ordnung $p - 1$. Dann gilt aber $\pmod{p}$

$$1 \equiv (a + bp)^{p-1} = a^{p-1} + (p-1) \cdot a^{p-2} bp + \sum_{i=2}^{p-1} \binom{p-1}{i} a^{p-1-i} b^i p^i$$

$$a^{p-1} - a^{p-2} bp \equiv 1 - a^{p-2} bp,$$

also müsste $a^{p-2} b$ durch p teilbar sein, Widerspruch. □

Lemme 2.6. *Sei p eine Primzahl und k eine natürliche Zahl mit $k \geq 2$ falls $p \geq 3$ bzw. $k \geq 3$ falls $p = 2$. Sei a teilerfremd zu p, dann gilt*

$$\left.\begin{aligned} \operatorname{ord}_{p^{k-1}}(a) &= (p-1)p^{m-1} \\ \operatorname{ord}_{p^k}(a) &= (p-1)p^m \end{aligned}\right\} \Longrightarrow \operatorname{ord}_{p^{k+1}}(a) = (p-1)p^{m+1}$$

Beweis. Nach Voraussetzung gilt $a^{(p-1)p^{m-1}} \equiv 1 \pmod{p^{k-1}}$ und $a^{(p-1)p^{m-1}} \not\equiv 1 \pmod{p^k}$. Daraus folgt

$$a^{(p-1)p^{m-1}} = 1 + bp^{k-1} \quad mit p \nmid b.$$

Nach Voraussetzung und Lemma 2.4 (c) ist $\operatorname{ord}_{p^{k+1}}(a)$ entweder gleich $(p-1)p^m$ oder gleich $(p-1)p^{m+1}$. Wir nehmen ersteres an und führen dies zu einem Widerspruch. Dann wäre nämlich

$$\begin{aligned} 1 \equiv (a^{(p-1)p^{m-1}})^p &= (1 + bp^{k-1})^p \\ &= 1 + p \cdot bp^{k-1} + \sum_{i=2}^{p} \binom{p}{i} b^i p^{i(k-1)} \pmod{p^{k+1}} \\ &\equiv 1 + bp^k. \end{aligned}$$

Dabei gilt die letzte Kongruenz, weil alle Terme in der Summe durch p^{k+1} teilbar sind : Für $i \geq 3$ folgt dies aus $i(k-1) \geq k+1$ wegen $k \geq 2$ und für $i = 2$ folgt dies aus $k \geq 3$ falls $p = 2$ und aus $p \mid \binom{p}{2}$ falls $p \geq 3$. Obige Kongruenz zeigt aber, dass b durch p teilbar sein muss, ein Widerspruch. □

Wir kommen nun zum Beweis von Satz 2.3 :

(c) Ist $k \geq 2$ und ist a eine primitive Wurzel modulo p^k , dann gilt $\mathrm{ord}_{p^{k-1}}(a) = (p-1)p^{k-2}$ und $\mathrm{ord}_{p^k}(a) = (p-1)p^{k-1}$. Also sind die Voraussetzungen von Lemma 2.6 für $m = k-1$ erfüllt und die Aussage desselben ist gerade, dass a auch eine primitive Wurzel modulo p^{k+1} ist. Die Behauptung folgt jetzt induktiv.

(a) Wir zeigen zunächst, dass in den Fällen (i) bis (iii) primitive Wurzeln existieren. Für (i) ist das klar. Für (ii) garantiert Satz 2.2 die Existienz einer solchen für p, Lemma 2.5 für p^2 und (c) für alle höheren Potenzen. Für (iii) beachte man $\varphi(2p^k) = \varphi(p^k)$. Somit ist jede ungerade primitive Wurzel modulo p^k auch eine solche modulo $2p^k$ (d.h. man wählt einfach eine primitive Wurzel modulo p^k und addiert gegebenenfalls p^k dazu).
Ist umgekehrt n nicht vom Typ (i)-(iii), dann ist n entweder eine 2er-Potenz ≥ 8 oder ein Produkt zweier teilerfremder Zahlen $n_1, n_2 \geq 3$. Im ersten Fall kann n keine primitive Wurzel besitzen, weil schon 8 keine hat. Im zweiten Fall sind $\varphi(n_1)$ und $\varphi(n_2)$ beide gerade und mit Lemma 2.4 (b) folgt für jede zu n teilerfremde Zahl a

$$\mathrm{ord}_n(a) = kgV(\mathrm{ord}_{n_1}(a), \mathrm{ord}_{n_2}(a)) \leq kgV(\varphi(n_1), \varphi(n_2)) < \varphi(n_1)\varphi(n_2) = \varphi(n).$$

Also ist a keine primitive Wurzel modulo n.

(d) Es gilt $\mathrm{ord}_8(5) = 2$ und $\mathrm{ord}_1\, 6(5) = 4$. Ähnlich wie im Beweis von (c) folgt daraus mit Lemma 2.6 induktiv $\mathrm{ord}_{2^k}(5) = 2^{k-2}$ für alle $k \geq 3$. Dies ist nach (a) ausserdem die grösstmögliche Ordnung. Wir zeigen als nächstes, dass $-1 \not\equiv 5^m \pmod{2k}$ gilt für alle m und alle $k \geq 2$. Sonst wäre nämlich sogar $1 \equiv 5^m \equiv 1 \pmod 4$, ein Widerspruch. Somit sind die 2^{k-1} Restklassen $\pm 5^m$ mit $0 \leq m < 2^{k-2}$ paarweise verschieden und müssen somit alle ungeraden Restklassen $\pmod{2^k}$ genau einmal durchlaufen.

(b) Aus Lemma 2.5 folgt sofort, dass *mindestens* $p-1$ der Zahlen $a, a+p, \ldots, a+(p-1)p$ primitive Wurzel modulo p^2 ist. Insgesamt gibt es aber $\varphi(\varphi(p)) = \varphi(p-1)$ primitive Wurzeln modulo p und $\varphi(\varphi(p^2)) = (p-1)\varphi(p-1)$ solche modulo p^2 , also *genau* $p-1$ mal so viele. Wären also für ein a wie oben alle p Zahlen primitive Wurzeln modulo p^2, dann gäbe es insgesamt zu viele davon, ein Widerspruch.

3 Divers

3.1 La partie entière

Pour un nombre réel x désigne $\lfloor x \rfloor$ le plus grand nombre entier $\leq x$. On a par exemple $\lfloor 5 \rfloor = 5$, $\lfloor -2.6 \rfloor = -3$ et $\lfloor \pi \rfloor = 3$. On appelle $\lfloor \cdot \rfloor$ la *partie entière* de x. L'entier $\lfloor x \rfloor$ est uniquement déterminé par les inéquations

$$\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1.$$

On peut les reformuler pour obtenir

$$x - 1 < \lfloor x \rfloor \leq x.$$

Pour un nombre réel x, $\{x\} = x - \lfloor x \rfloor$ désigne la *partie fractionnaire* de x. On a par exemple $\{-3.1\} = 0.9$, $\{\pi\} = 0.1415\ldots$, en particulier $\{x\} \geq 0$ avec égalité si et seulement si x est un nombre entier.

Une observation importante pour la résolution de problèmes traitant de parties entières est la suivante : entre deux entiers consécutifs il n'y en a pas d'autres. Cela nous donne le résultat suivant :

Exemple 16. *Soient α et β deux nombres positifs* irrationnels *avec $\frac{1}{\alpha} + \frac{1}{\beta} = 1$. Alors les suites $\lfloor \alpha m \rfloor$ et $\lfloor \beta n \rfloor$ contiennent chaque nombre naturels exactement une fois à eux deux.*

Solution. Commençons par montrer que les suites sont disjointes. Supposons qu'il existe m et n naturels avec $\lfloor \alpha m \rfloor = \lfloor \beta n \rfloor = q$. Alors $q < \alpha m < q+1$, tout comme $q < \beta \mathrm{n} < q+1$, avec des inégalités strictes car α et β sont irrationnels. Par conséquent

$$\frac{m}{q+1} < \frac{1}{\alpha} < \frac{m}{q}, \qquad \frac{n}{q+1} < \frac{1}{\beta} < \frac{n}{q}.$$

En additionnant les inéquations on obtient

$$\frac{m+n}{q+1} < 1 < \frac{m+n}{q} \quad \Rightarrow \quad q < m+n < q+1,$$

ce qui est impossible. Ainsi $\lfloor \alpha m \rfloor \neq \lfloor \beta n \rfloor$.
Nous allons maintenant montrer que chaque nombre naturel apparaît dans une des suites. Supposons que q ne soit dans aucune des suites. Il existe alors deux entiers non-négatifs m et n avec

$$\alpha m < q < q+1 < \alpha(m+1), \qquad \beta n < q < q+1 < \beta(n+1). \frac{m}{q} < \frac{1}{\alpha} < \frac{m+1}{q+1}, \qquad \frac{n}{q} < \frac{1}{\beta} < \frac{n+1}{q+1}.$$

En additionnant ces inéquations on obtient

$$\frac{m+n}{q} < 1 < \frac{m+n+2}{q+1} \quad \Rightarrow \quad m+n < q < q+1 < m+n+2.$$

Contradiction car entre $m+n$ et $m+n+2$ il n'y a de la place que pour un seul entier. □

Exemple 17. *Montrer que la suite* $a_n = \lfloor n + \sqrt{n} + 1/2 \rfloor$ *contient tous les nombres naturels à l'exception des carrés.*

Solution. Supposons qu'il existe un m qui n'apparaît pas dans la suite monotone a_n. Il existe alors un nombre naturel n avec

$$n + \sqrt{n} + \frac{1}{2} < m < m + 1 < n + 1 + \sqrt{n+1} + \frac{1}{2}.$$

il s'ensuit alors, dans l'ordre

$$\begin{aligned} & \sqrt{n} < m - n - \frac{1}{2} < \sqrt{n+1} \\ \Rightarrow \quad & n < (m-n)^2 - (m-n) + \frac{1}{4} < n + 1 \\ \Rightarrow \quad & n - \frac{1}{4} < (m-n)^2 - (m-n) < n + \frac{3}{4}, \end{aligned}$$

et donc $(m-n)^2 - (m-n) = n$, ainsi $m = (m-n)^2$ est un carré. Un simple argument calculatoire nous permet de terminer la preuve. Il existe exactement k carrés positifs $\leq k^2+k$ et exactement k^2 nombres de la forme $\lfloor n+\sqrt{n}+1/2 \rfloor$. Par conséquent $\lfloor n+\sqrt{n}+1/2 \rfloor$ est le n-ième nombre non carré. □

Il existe quelques grandeurs qui sont faciles à décrire à l'aide des parties entières.

— La quantité de nombres naturels $\leq n$ divisibles par a vaut $\left\lfloor \frac{n}{a} \right\rfloor$.

— Soit p un nombre premier. La plus grande puissance à laquelle p divise $n!$ vaut

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots$$

car il existe exactement $\left\lfloor \frac{n}{p} \right\rfloor$ multiples de p plus petits que n. Chacun de ces nombres apporte un facteur p à la décomposition en nombres premiers de $n!$. Or exactement $\left\lfloor \frac{n}{p^2} \right\rfloor$ de ces nombres sont divisibles par p^2 également et apportent encore un facteur p, etc.

La partie entière n'est bien entendu pas additive, c'est-à-dire qu'en général $\lfloor x + y \rfloor \neq \lfloor x \rfloor + \lfloor x \rfloor$. Nous avons toutefois l'importante identité d'Hermite :

Théorème 3.1. *Pour tout nombre entier* n *et tout réel* x *on a*

$$\lfloor nx \rfloor = \lfloor x \rfloor + \left\lfloor x + \frac{1}{n} \right\rfloor + \left\lfloor x + \frac{2}{n} \right\rfloor + \dots + \left\lfloor x + \frac{n-1}{n} \right\rfloor.$$

Preuve. Choisissons un k tel que $\frac{k}{n} \leq \{x\} < \frac{k+1}{n}$. Le côté gauche vaut alors $n\lfloor x \rfloor + k$. Du côté droit les premiers $n-k$ termes de la somme valent $\lfloor x \rfloor$, les k autres $\lfloor x \rfloor + 1$. d'où l'affirmation. □