Chandan Singh DALAWAT

Wilson’s theorem

<http://jtnb.cedram.org/item?id=JTNB_2009__21_3_517_0>

© Université Bordeaux 1, 2009, tous droits réservés.

L’accès aux articles de la revue « Journal de Théorie des Nombres de Bordeaux » (http://jtnb.cedram.org/), implique l’accord avec les conditions générales d’utilisation (http://jtnb.cedram.org/legal/). Toute reproduction en tout ou partie cet article sous quelque forme que ce soit pour tout usage autre que l’utilisation à fin strictement personnelle du copiste est constitutive d’une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.
Wilson’s theorem

par CHANDAN SINGH DALAWAT

Résumé. On fait voir comment K. Hensel aurait pu étendre le théorème de Wilson de ℤ à l’anneau des entiers ℓ d’un corps de nombres, pour trouver le produit de tous les éléments inversibles d’un quotient fini de ℓ.

Abstract. We show how K. Hensel could have extended Wilson’s theorem from ℤ to the ring of integers ℓ in a number field, to find the product of all invertible elements of a finite quotient of ℓ.

1. Introduction

...puisque de tels hommes n’ont pas cru ce sujet indigne de leurs méditations... [1].

More than two hundred years ago, Gauss generalised Wilson’s theorem \((p-1)! \equiv -1 \pmod{p}\) for a prime number \(p\) to an arbitrary integer \(A > 0\) in §78 of his Disquisitiones:

**Theorem 1.1.** ([1]) *Poductum ex omnibus numeris, numero quocunque dato A minoribus simulque ad ipsum primis, congruum est secundum A, unitati vel negatiue vel positiue sumtae.*

(The product of all elements in \((\mathbb{Z}/A\mathbb{Z})^\times\) is \(-1\) or \(-1\)). He then specifies that the product in question is \(-1\) if \(A\) is 4, or \(p^m\), or \(2p^m\) for some odd prime \(p\) and integer \(m > 0\); it equals 1 in the remaining cases.

According to Gauss ([1], §76) the elegant theorem according to which “upon augmenting the product of all numbers less than a given prime number by the unity, it becomes divisible by that prime number” was first stated by Waring in his Meditationes — which appeared in Cambridge in 1770 — and attributed to Wilson, but neither could prove it. Waring remarks that the proof must be all the more difficult as there is no notation which might express a prime number. *Nach unserer Meinung aber müssen derartige Wahrheiten vielmehr aus Begriffen (notionibus) denn aus Bezeichnungen (notationibus) geschöpft werden* [1]. The first proof was given by Lagrange (1771).

Manuscrit reçu le 4 avril 2008.
Some hundred years later, Hensel [2] developed his local notions, which could have allowed him to extend the result from \( \mathbb{Z} \) to rings of integers in number fields; our aim here is to show how he could have done it.

**Proposition 1.1.** ("Wilson's theorem") For an ideal \( \mathfrak{a} \subset \mathfrak{o} \) in the ring of integers of a number field \( K \), the product of all elements in \( (\mathfrak{o}/\mathfrak{a})^\times \) is 1, except that it is

1. \(-1\) when \( \mathfrak{a} \) has precisely one odd prime divisor, and \( v_p(\mathfrak{a}) < 2 \) for every even prime ideal \( p \).
2. \(1 + \pi \) (resp. \(1 + \pi^2\)) when all prime divisors of \( \mathfrak{a} \) are even and for precisely one of them, say \( p \), \( v_p(\mathfrak{a}) > 1 \) with moreover \( v_p(\mathfrak{a}) = 2 \), \( f_p = 1 \) (resp. \( v_p(\mathfrak{a}) = 3 \), \( f_p = 1 \), \( e_p > 1 \)); here \( \pi \) is any element of \( p \) not in \( p^2 \), and we have indentified \( (\mathfrak{o}/p^2)^\times \) (resp. \( (\mathfrak{o}/p^3)^\times \)) with a subgroup of \( (\mathfrak{o}/\mathfrak{a})^\times \).

The notation and the terminology are unambiguous: a prime ideal \( p \) of \( \mathfrak{o} \) is even if \( 2 \in p \), odd if \( 2 \not\in p \); \( v_p(\mathfrak{a}) \) is the exponent of \( p \) in the prime decomposition of \( \mathfrak{a} \); \( f_p \) is the residual degree and \( e_p \) the ramification index of \( K_p|Q_p \) (\( p \) being the rational prime which belongs to \( p \)).

(\(1 + \pi = 1 \) in \( (\mathfrak{o}/p^2)^\times \) (resp. \(1 + \pi^2 = 1 \) in \( (\mathfrak{o}/p^3)^\times \)) for some even prime \( p \subset \mathfrak{o} \). Example: \( \mathfrak{o} = \mathbb{Z} \) (resp. \( \mathbb{Z}[\sqrt{2}] \)) and \( p \) the unique even prime of \( \mathfrak{o} \). More banally, we have \(-1 = 1 \) in \( (\mathfrak{o}/p^n)^\times \) when \( p \) is an even prime and \( n \) is between 1 and \( e_p \).)

2. \( d_2 \)

The elementary observation behind the proof of Gauss’s th. 1.1, also used in our proof of prop. 1.1, is that the sum \( s \) of all the elements in a finite commutative group \( G \) is 0, unless \( G \) has precisely one order-2 element \( \tau \), in which case \( s = \tau \). Anyone can supply a proof; he can then skip this section, and take the condition “\( d_2(G) = 1 \)” as a shorthand for “\( G \) has precisely one order-2 element.”

Define \( d_2(G) = \dim_{F_2}(2G) \), where \( 2G \) is the subgroup of \( G \) killed by 2. It is clear that \( G \) has \( 2^{d_2(G)} - 1 \) order-2 elements.

**Example.** For a prime number \( p \) and a positive integer \( n \), we have \( d_2((\mathbb{Z}/p^n\mathbb{Z})^\times) = \)

1. 1 if \( p \neq 2 \),
2. 0 if \( p = 2 \) and \( n = 1 \),
3. 1 if \( p = 2 \) and \( n = 2 \),
4. 2 if \( p = 2 \) and \( n > 2 \).

In this example, the unique order-2 element is \(-1 \) whenever \( d_2 = 1 \).

**Lemma 2.1.** The sum \( s \) of all elements in \( G \) is 0 unless \( d_2(G) = 1 \), in which case \( s \) is the unique order-2 element of \( G \).
The involution \( \iota : g \mapsto -g \) fixes every element of the subgroup \( 2G = \text{Ker}(x \mapsto 2x) \). As the sum of elements in the remaining orbits of \( \iota \) is 0, we are reduced to the case \( G = 2G \) of a vector \( F_2 \)-space, and the proof is over by induction on the dimension \( d_2(G) \) of \( 2G \), starting with dimension 2.

**Proof of Gauss’s th. 1.1** : Let \( A = \prod_p p'^{m_p} \) be the prime decomposition of \( A \). By the Chinese remainder theorem, \( (\mathbb{Z}/AZ)^\times \) is the product over \( p \) of \( (\mathbb{Z}/p'^{m_p}Z)^\times \), so \( d_2((\mathbb{Z}/AZ)^\times) \) is the sum over \( p \) of \( d_2((\mathbb{Z}/p'^{m_p}Z)^\times) \). In view of the foregoing Example, the only way for this sum to be 1 is for \( A \) to be \( 2^2 \), or \( p'^{m_p} \), or \( 2p'^{m_p} \) for some odd prime \( p \) and integer \( m_p > 0 \).

### 3. Local units

Let’s enter Hensel’s world : let \( p \) be a prime number, \( K \mid \mathbb{Q}_p \) a finite extension, \( \mathfrak{o} \) its ring of integers, \( \mathfrak{p} \) the unique maximal ideal of \( \mathfrak{o} \). Let \( n > 0 \) be an integer. We would like to know when \( d_2((\mathfrak{o}/p^n)^\times) = 1 \), and, when such is the case, which one the unique order-2 element is.

**Proposition 3.1.** Denoting by \( e \) the ramification index and by \( f \) the residual degree of \( K \mid \mathbb{Q}_p \), we have \( d_2((\mathfrak{o}/p^n)^\times) = \)

1. \( 1 \) if \( p \neq 2 \),
2. \( 0 \) if \( p = 2, n = 1 \),
3. \( 1 \) if \( p = 2, n = 2, f = 1 \),
4. \( 1 \) if \( p = 2, n = 3, f = 1, e > 1 \),
5. \( > 1 \) in all other cases.

For any \( \mathfrak{o} \)-basis \( \pi \) of \( \mathfrak{p} \), the unique order-2 element in the cases \( d_2 = 1 \) is

1. \( -\bar{1} \) if \( p \neq 2 \),
2. \( \bar{1} + \bar{\pi} \) if \( p = 2, n = 2, f = 1 \),
3. \( \bar{1} + \bar{\pi}^2 \) if \( p = 2, n = 3, f = 1, e > 1 \).

**Proof :** For every \( j > 0 \), denote by \( U_j \) the kernel of \( \mathfrak{o}^\times \to (\mathfrak{o}/p^j)^\times \). If \( p \neq 2 \), the group \( (\mathfrak{o}/p^n)^\times \) is the direct product of the even-order cyclic group \( (\mathfrak{o}/p)^\times \) and the \( p \)-group \( U_1/U_n \), so \( d_2 = 1 \).

Assume now that \( p = 2 \). When \( n = 1 \), the group \( (\mathfrak{o}/p)^\times \) is (cyclic) of odd order, so \( d_2 = 0 \). If \( f > 1 \), then the \( d_2 \) of \( U_1/U_2 \) is \( f \) and hence the \( d_2 \) of \( (\mathfrak{o}/p^n)^\times \) is \( > 1 \) for every \( n > 1 \).

Assume further that \( f = 1 \). When \( n = 2 \), the \( d_2 \) of \( (\mathfrak{o}/p^2)^\times = U_1/U_2 \) is \( f = 1 \). If moreover \( e = 1 \), then the \( d_2 \) of \( U_1/U_n \) is 2 for \( n > 2 \) (see Example).

Assume finally that, in addition, \( e > 1 \). We see that \( U_1/U_3 \) is generated by \( \bar{1} + \bar{\pi} \), since \((1 + \pi)^2 = 1 + \pi^2 + 2\pi \) is in \( U_2 \) but not in \( U_3 \). However, \( U_1/U_4 \) is not cyclic because its order is 8 whereas every element has order at most 4 : for every \( a \in \mathfrak{o} \),

\[
(\bar{1} + a\bar{\pi})^4 = \bar{1} + 4\bar{\pi}a + 6\bar{\pi}^2a^2 + 4\bar{\pi}^3a^3 + \bar{\pi}^4a^4 = \bar{1}
\]

(For $p = 2$ and $n > 2e$, we have $d_2((\mathfrak{o}/p^n)^\times) = 1 + ef$ ; cf. Hasse, *Zahlentheorie*, Kap. 15.)

**Corollary 3.1.** The only cases in which the group $(\mathfrak{o}/p^n)^\times$ has precisely one order-2 element $s$ are : $p \neq 2$ ; $p = 2$, $n = 2$, $f = 1$ ; $p = 2$, $n = 3$, $f = 1$, $e > 1$. In these three cases, $s = -\bar{1}$, $\bar{1} + \bar{\pi}$, $\bar{1} + \bar{\pi}^2$, respectively. The group $(\mathfrak{o}/p^n)^\times$ has no order-2 element precisely when $p = 2$, $n = 1$.

### 4. The proof

Let us return to the global situation of an ideal $\mathfrak{a} \subset \mathfrak{o}$ in the ring of integers of a number field $K | \mathbb{Q}$. The proof can now proceed as in the case $\mathfrak{o} = \mathbb{Z}$ (§2). Everything boils down to deciding if the $d_2$ of $(\mathfrak{o}/\mathfrak{a})^\times$ is 1 — we know that the product of all elements is 1 if $d_2 \neq 1$ (lemma 2.1). Writing $\mathfrak{a} = \prod_p \mathfrak{p}^{m_p}$ the prime decomposition of $\mathfrak{a}$, the Chinese remainder theorem tells us that $d_2((\mathfrak{o}/\mathfrak{a})^\times)$ is the sum, over the various primes $p$ of $\mathfrak{o}$, of $d_2((\mathfrak{o}/\mathfrak{p}^{m_p})^\times)$. This sum can be 1 only when one of the terms is 1, the others being 0.

For each $p$, the group $(\mathfrak{o}/\mathfrak{p}^{m_p})^\times$ is the same as $(\mathfrak{o}_p/\mathfrak{p}_p^{m_p})^\times$, where $\mathfrak{o}_p$ is the completion of $\mathfrak{o}$ at $p$ and $\mathfrak{p}_p$ is the unique maximal ideal of $\mathfrak{o}_p$. Running through the possibilities enumerated in prop. 3.1 completes the proof of prop. 1.1.

**Example.** Let $\zeta \in \overline{\mathbb{Q}}^\times$ be an element of order $2^t$ ($t > 1$) ; take $K = \mathbb{Q}(\zeta)$ and $\mathfrak{p}$ the unique even prime of its ring of integers $\mathbb{Z}[\zeta]$. We have $e_p = 2^{t-1}$ and $f_p = 1$ ; we may take $\pi = 1 - \zeta$. The product of all elements in $(\mathbb{Z}[\zeta]/p^n)^\times$ is respectively $\bar{1}$, $\bar{1} + \bar{\pi}$, $\bar{1} + \bar{\pi}^2$, $\bar{1}$ for $n = 1$, $n = 2$, $n = 3$ and $n > 3$.

### 5. Acknowledgements

We thank Herr Prof. Dr. Peter Roquette for suggesting the present definition $d_2(G) = \dim_{\mathbb{F}_2}(2G)$ instead of the original $d_2(G) = \dim_{\mathbb{F}_2}(G/2G)$. After this Note was completed, a search in the literature revealed M. Laššák, *Wilson’s theorem in algebraic number fields*, Math. Slovaca, 50 (2000), no. 3, pp. 303–314. We solicited a copy from Prof. G. Grekos, and thank him for supplying one ; it contains substantially the same result as our prop. 1.1. Our proof is shorter, simpler, more direct, and more conceptual ; it is based on *notonibus* rather than *notationibus*, of which there is now-a-days a surfeit. In any case, our aim was to show how Hensel could have proved prop. 1.1.
Wilson’s theorem

References


Chandan Singh Dalawat
Harish-Chandra Research Institute
Chhatnag Road, Jhunsi
211019 Allahabad, Inde
E-mail: dalawat@gmail.com