Department of Philosophy - Utrecht University

Euler's φ-function in the context of $I\Delta_0$

M.D. Jumelet

Logic Group
Preprint Series
No. 108
March 1994

Utrecht Research
Institute for
Philosophy

ISBN 90-393-0572-2
ISSN 0929-0710
Dr. A. Visser, Editor

Euler's φ-function in the context of $I\Delta_0$.

Marc Jumelet
Department of Philosophy,
Utrecht University
Heidelberglaan 8
3584 CS Utrecht
e-mail: Marc.Jumelet@phil.ruu.nl

Abstract. It is demonstrated that we can represent Euler's φ-function by means of a Δ_0-formula in such a way that the theory $I\Delta_0$ proves the recursion equations that are characteristic for this function.

§1. Introduction. The theory $I\Delta_0$, that is, the theory of arithmetic which has as its axioms those that define the properties of a discretely ordered semiring as well as induction axioms for those formulas that contain bounded quantifiers only, has been the object of study for a variety of mathematical aspects. It has been studied for its mathematical strength, its metamathematical properties (often with the addition of axioms that ascertain the totality of certain rapidly growing functions to make reasoning about objects of metamathematical character possible) and its purely syntactical abilities, notably, as a proof system. In the following we will treat a problem concerning the possibility of defining a classical number theoretical function.

It is known for quite a long time already that a Δ_0-definition for the exponentiation function exists, in the sense that we have a Δ_0-formula $EXP(x, y, z)$ such that the formulas $EXP(0, S0, z)$, $\forall x, y_1, y_2\ EXP(x, y_1, z) \wedge EXP(x, y_2, z) \rightarrow y_1 = y_2$ as well as the formula that articulates the specific recursion property of exponentiation, that is $\forall x, y\ EXP(x, y, z) \rightarrow EXP(Sx, z.y, z)$, become provable in $I\Delta_0$. It is due to this result that the theory $I\Delta_0$ can handle finite sequences by means of binary coding. This kind of coding can be used for syntactical purposes such as the construction of a proof predicate, a truth predicate, or any other type of syntactical object, or the construction of predicates that represent the counting of certain sets that are themselves described by Δ_0-formulas. As to the last case, the picture that is emerging about the possibility to find formulas that represent the counting of Δ_0-sets, gives rise to the idea that either these sets should be very small in the sense that for every number n, the amount of elements smaller than that number is in logarithmic proportion with respect to that number (in order to make sure that a formula that "counts" by constructing the code of a bijection between the subset of n of elements that satisfy the Δ_0-predicate under consideration and the ordinal that represents the size of this subset does not necessarily use values for codes that might become too large, see Paris & Wilkie [3]), or they should be described by means of very simple Δ_0-formulas, expressing rather trivial properties.

Traditionally, coding syntax was performed by means of a different kind of coding, the one that is based on the Chinese Remainder Theorem. It is rather hard to judge in general

under which circumstances we should prefer binary coding to number theoretical coding like the one in which the Chinese Remainder Theorem is used as a coding device.

§2. Result. We will give an example of a well-known function that can most easily be computed with the help of the Chinese Remainder Theorem, whereas a computation of its values by means of a binary coding procedure alone might be a lot more complicated. The function we have in mind is Euler's φ-function that assigns to a number $n \in \mathbb{N}$ the cardinality of the set $\{m<n \mid \gcd(n, m) = 1\}$. We will prove the following theorem:

THEOREM. 2.1. There is a Δ_0-formula $\varphi(x, y)$ such that $I\Delta_0$ proves the following clauses that articulate the recursion equations for Euler's φ-function:
i. "$\varphi(x, y)$ defines a total function";
ii. "$\varphi(0, 0)$ and $\varphi(1, 1)$ hold";
iii. "for all m, p if p is a prime divisor of m and r is such that $r.p=m$, then, if not $p^2|m$ and $\varphi(r, s)$ holds, this will imply $\varphi(m, (p-1).s)$ and if $p^2|m$, then $\varphi(m, p.s)$ holds".

These are recursion equations that we have to verify to be sure that the constructed formula $\varphi(x, y)$ behaves the way it should. Note that we immediately get that $I\Delta_0$ proves for all prime numbers $p>1$: $\varphi(p, p-1)$. As we said above, we will construct the formula $\varphi(x, y)$ by means of the Chinese Remainder Theorem.

Intuitively, the construction is as follows. Let a number x be given. Let furthermore

$$x = \prod_{p|x} p^{v_p(x)}$$

be the decomposition of x in prime factors. What $I\Delta_0$ needs to be able to construct is the number

$$z_x = \prod_{p|x} (p-1)$$

because the construction of the number

$$y_x = \prod_{p|x} p^{v_p(x)-1}$$

is rather unproblematic and it is the value $z_x.y_x$ that we are looking for. We will use the fact that there exists a prime decomposition of this number z_x and that we know an upper bound for the prime numbers that may divide z_x because clearly all primes that possibly divide this number are smaller than the greatest prime number that divided x. For this reason we only have to know their exponents in the decomposition of z_x. We recall the

following theorem of Legendre (cf. Smoryński [5]) that will help us to find the necessary bound on these exponents: if p is a prime number, then, for any number n, the following holds:
if α is the greatest number such that p^α divides $n!$, then $\alpha = \frac{n-\#_p n}{p-1}$, where $\#_p n$ denotes the sum of the coefficients in the representation of n in base p.

Because we only need parts of this theorem, we will reformulate these in terms which the theory $I\Delta_0$ can handle. Let from now on $v_p(x)$ be an expression for a Δ_0-function which assigns to a number x the exponent of p in the greatest power of p that divides x and let $\#_p x$ be an expression for a Δ_0-function which assigns to a number x the sum of the coefficients in the representation of x in base p. It may be stressed at this point that we can safely assume these notions to be described by Δ_0-formulas about which $I\Delta_0$ proves that they actually define total functions and that they respect the obvious recursion equations. As to the computation of the sum of coefficients in the representation of a number in a certain base, this assumption is perfectly justified for the representation of a number in base 2 if we inspect Hájek & Pudlák [2]. A Δ_0-formula for the sum of the coefficients for an arbitrary base p can be deduced from the one for the representation in base 2 by formalizing a simple "divide and conquer" algorithm. In general, the fact that these expressions exist allows us to use them as functions. In this way, we obtain the following proposition.

PROPOSITION 2.2. $I\Delta_0$ proves:
i. $\forall p\ \forall x\ [x - \#_p x + (p - 1).\ v_p(x + 1) = (x + 1) - \#_p(x + 1)]$;
ii. $\forall p\ \forall x, y\ [y \geq 1 \rightarrow (x - \#_p x + (p - 1).v_p(x + y) \leq (x + y) - \#_p(x + y))]$;
iii. $\forall p\ \forall x\ [(p - 1).\ v_p(x) \leq (x + 1) - \#_p(x + 1)]$.

This is, in a manner of speaking, a formulation of what $I\Delta_0$ understands about Legendre's theorem above. If p is taken to be a prime number then i above takes the form of the recursion equation of the summation that is implicit in Legendre's theorem.

PROOF. The second proposition follows from the first one, as can be deduced with the following kind of induction (on y): fix x and p. If $y = 1$, then i already settles ii. If $y \neq 1$, then distinguish two cases. The first one is the one in which $v_p(x + y) = 0$. We now get:

$$\begin{aligned} x - \#_p x + (p - 1).\ v_p(x + y + 1) &= x - \#_p x + (p - 1).(v_p(x + y + 1) + v_p(x + y)) \\ &\leq (x + y) - \#_p(x + y) + (p - 1).v_p(x + y + 1) \\ &= (x + y + 1) - \#_p(x + y + 1). \end{aligned}$$

This last line follows by i.

The second case is the one in which $v_p(x + y) \neq 0$, which is equivalent to saying that p divides $x + y$. In this situation we obtain our bound by:

$$\begin{aligned} x - \#_p x + (p - 1).\, v_p(x + y + 1) &= x - \#_p x \\ &\leq x - \#_p x + (p - 1).v_p(x + y) \\ &\leq (x + y) - \#_p(x + y) \\ &= (x + y + 1) - \#_p(x + y + 1). \end{aligned}$$

Notice that all quantifiers hidden in this proof occur bounded and that the reasoning takes place entirely inside $I\Delta_0$.

For i we have a similar construction. Reason in $I\Delta_0$ and fix a number p. The proof is by Δ_0-induction. If $x = 0$, then $v_p(x + 1) = 0$, $\#_p x = 0$ and also $\#_p(x + 1) = 1$, so there is very little to do. If $x \neq 0$, we proceed by induction as follows: let y, r be such that $0 \leq r < p$ and that $x = y.p + r$ is the case. We will distinguish two cases.

1. $r + 1 = p$. In this situation we obtain:

$$\begin{aligned} x - \#_p x + (p - 1).\, v_p(x + 1) &= (y.p + r) - \#_p(y.p + r) + (p - 1).\, v_p(y.p + r + 1) \\ &= (y.p + r) - (\#_p(y) + r) + (p - 1).\, v_p(y.p + p) \\ &= y.p - \#_p(y) + (p - 1).\, (1 + v_p(y + 1)) \\ &= (p - 1).(y + 1) + (y + 1) - \#_p(y + 1) \\ &\quad \text{(by } \Delta_0\text{-induction)} \\ &= p.(y + 1) - \#_p(p.(y + 1)). \end{aligned}$$

That is what we had to show.

2. $r + 1 \neq p$. In this situation p will not divide $x + 1$, so:

$$\begin{aligned} x - \#_p x + (p - 1).\, v_p(x + 1) &= (y.p + r) - \#_p(y.p + r) + (p - 1).\, 0 \\ &= (y.p + r + 1) - \#_p(y.p + r + 1). \end{aligned}$$

As to iii, we remark that if we take $x = 1$ and $y = x - 1$ in ii, then we get:

$$(p - 1).\, v_p(x) \leq x - \#_p x,$$

and thus, by i:

$$(p - 1).\, v_p(x) \leq (x + 1) - \#_p(x + 1).$$

This concludes the proof.

In passing we note that, with the same equipment as above, one can deduce by means of simple inductive calculations, the assertion: $\#_p x + \#_p y \geq \#_p(x + y)$, for all x, y and $p \neq 1$. This assertion, in combination with Legendre's theorem, is easily recognised as the logarithmic analogue of the theorem that states that the binomial coefficients are integers. This latter fact can not be properly expressed with respect to the theory $I\Delta_0$, simply because this theory does not prove the totality of the binomial function.

In our present situation, we can benefit from Legendre's theorem by observing that if q^β is the greatest power of a prime number q that divides z_x in the situation above, then q

must necessarily be smaller than the greatest prime number, say p_m, that divided x, and so q^β will also divide $p_m!$, so it must be the case that $\beta \leq \frac{p_m - \#_q p_m}{q-1} < p_m$. This is the place where the finite sequences come in. In order to find the prime decomposition of z_x we construct, for every prime number $q<p_m$, a finite sequence $<\beta_i>$ for i such that $p_i^{\alpha_i} | x \,\&\, \neg p_i^{\alpha_i+1} | x \,\&\, p_i^{\alpha_i} \neq 1$, that is, a sequence of length equal to the cardinality of the set of prime divisors of x, in such a way that

$$\beta_i = \sum_{r \leq p_i \; r \text{ prime } r|x} v_q(r-1),$$

where $v_q(r-1)$ denotes the exponent of the greatest power of q dividing $r-1$. These are the sequences that we will code by means of the Chinese Remainder Theorem.

Throughout the following construction we will assume that exponentiation as well as other, less complicated notions, like the property of being a prime number or the greatest or smallest prime divisor of a given number, can faithfully be represented by means of Δ_0-formulas. Furthermore, we will use the number theoretic notation $x \equiv y \bmod z$ with the meaning "z is a divisor of the absolute value of the difference of x and y".

Since we need to be able to use the Chinese Remainder Theorem, we will first state an obvious version of the prime decomposition theorem for $I\Delta_0$.

PROPOSITION 2.3. $I\Delta_0$ proves the following:
$\forall x \, \forall \, a, a' < x \, (a = a' \leftrightarrow \forall p \leq x \, (\text{"}p \text{ prime"} \wedge p|x \; \rightarrow a \equiv a' \bmod p^{v_p(x)}))$.

PROOF. The proof is by straightforward induction in $I\Delta_0$, as we shall now see. Instead of the statement above we will prove an equivalent statement, namely:

$\forall x \, \forall \, b < x \, (\forall p \leq x \, (\text{"}p \text{ prime"} \wedge p|x \; \rightarrow p^{v_p(x)} | b) \rightarrow b = 0)$.

The cases $x = 0$ and $x = 1$ are trivial. Let x be greater than 2 and fix $b < x$. We can now write $x = y.\, q^{v_q(x)}$ for the greatest prime number q that divides x. In this situation, if we have $\forall p \leq x \, (\text{"}p \text{ prime"} \wedge p|x \; \rightarrow p^{v_p(x)} | b)$, then we must also have, for suitable c such that $b = c.q^{v_q(x)}$ holds (which, in its turn, implies $c < y$):

$\forall p \leq y (\text{"}p \text{ prime"} \wedge p|y \; \rightarrow p^{v_p(y)} | c)$.

But, by induction, this implies: $c = 0$. Hence *a fortiori*: $b = 0$.

Notice that this theorem can also be formulated without using the functional notation for the exact exponent of a prime number dividing a certain number. This rather trivial proposition is needed in the construction to ensure that the Chinese Remainder Theorem can be used as a coding device.

Let $SP(x, p, q)$ denote the notion of consecutive prime divisors of x, that is:

DEFINITION 2.4.

$SP(x, p, q) := (\text{“}p, q \text{ prime”} \wedge p<q \wedge p|x \wedge q|x \wedge$
$\neg(\exists r \text{ “}r \text{ prime”} \wedge r|x \wedge p<r \wedge r<q))$.

We will use the predicate $A(x, p, \beta)$ to describe the greatest number β such that p^β divides z_x:

DEFINITION 2.5.

$A(x, p, \beta) :=$ “p prime”$\wedge$
$\exists a<x[\exists q \leq x(\text{“}q \text{ least prime divisor of } x\text{”} \wedge a \equiv v_p(q\text{-}1) \bmod q^{v_q(x)})$
$\wedge \forall q, r(SP(x, q, r) \rightarrow \forall \gamma(a \equiv \bmod q^{v_q(x)} \leftrightarrow a \equiv \gamma + v_p(r\text{-}1) \bmod r^{v_r(x)})$
$\wedge \exists s(\text{“}s \text{ greatest prime divisor of } x\text{”} \wedge \beta \equiv a \bmod s^{v_s(x)} \wedge \beta<s^{v_s(x)})]$.

The number a in the definition above is the sequence that witnesses for each q such that q is a prime number that divides x the sum of the exponents β of p for each prime number r smaller than or equal to q that divides x such that p^β is the greatest power of p that divides the number r-1.

We can define the predicate $Z(z_x, x)$ as follows:

DEFINITION 2.6.

$Z(z_x, x) :=$ $(x \neq 1 \wedge \forall p, \beta \leq z_x[v_p(z_x) = \beta \leftrightarrow A(x, p, \beta)]) \vee (x = y = 1)$.

This predicate defines the number z_x by giving (by means of a Δ_0-formula) the exact form of its prime decomposition. This is unproblematic because, as we remarked above, all prime numbers that have to be taken into account as possible divisors of z_x are strictly smaller than the greatest prime number that divides x itself. This fact is already implicit in the definition of the predicate $A(x, y, z)$.

The predicate $Y(y_x, x)$ needed to define the other factor can be defined with the following formula:

DEFINITION 2.7.

$Y(y_x, x) := y_x|x \wedge \forall p < x[\text{“}p \text{ prime”} \wedge p|x \rightarrow (v_p(y_x) + 1 = v_p(x))]$.

Now we define the predicate $\varphi(x, y)$ as:

DEFINITION 2.8.

$\varphi(x, y) := \exists y_x, z_x \leq y\ (Z(z_x, x) \wedge Y(y_x, x) \wedge y = y_x.z_x) \vee (x = y = 0)$.

All these definitions clearly use Δ_0-formulas only. It requires some patience to verify the recursion equations cited above. As indicated there, it is the numbers z_x that cause some difficulty, so we will concentrate on them. We will therefore show that the following holds.

PROPOSITION 2.9. $I\Delta_0$ proves the following theorems:
i. "$A(x, y, z)$ defines a possibly partial function with arguments x, y",
ii. "if x is of the form q^n for q prime and p is prime, then $A(x, p, z)$ holds iff $v_p(q\text{-}1) = z$.
iii. "if x is of the form $p_m{}^n.r$ where p_m is the greatest prime number dividing x and $gcd(p_m, r) = 1$, then for any prime number $p < p_m$, for γ, δ such that
$A(r, p, \gamma)$ and $A(p_m{}^n, p, \delta)$: $A(x, p, \beta)$ iff $\beta = \gamma + \delta$",
iv. "if x is of the form q^n for q prime, then $Z(z_x, x)$ holds iff $z_x = q\text{-}1$",
v. "if $x = s.t$ and $gcd(s, t) = 1$ and $Z(z_s, s)$ and $Z(z_t, t)$, then $Z(z_x, x)$ iff
$z_x = z_s.z_t$".

We will now turn to the proof of this proposition. Some parts of this proof are merely sketches of what the exact proof in $I\Delta_0$ should be. For instance, the verification of the lemma's above relies heavily on the trustworthy conduct of functions like exponentiation and the ones that provide the sum of the coefficients of a number represented in a certain base.

PROOF. Throughout the following we will be reasoning in $I\Delta_0$.
i. Assume that $A(x, y, z)$ and $A(x, y, z')$ hold with $z \neq z'$. We will derive a contradiction as follows. Apparently, there are sequences $a < x$ and $a' < x$ such that $z \equiv a \bmod p_m{}^{\alpha_m}$ and $z' \equiv a' \bmod p_m{}^{\alpha_m}$ for p_m being the greatest prime number dividing x. So, $a \neq a'$. Therefore, by proposition 2.3 above, there is a least p_i prime dividing x such that $v_{p_i}(x) = \alpha_i$ and $a \not\equiv a' \bmod p_i{}^{\alpha_i}$. If this p_i is the smallest prime divisor of x, then $a \equiv \gamma \equiv a' \bmod p_i{}^{\alpha_i}$, where $v_y(p_i\text{-}1) = \gamma$, so that can simply not be the case. Evidently there have to be two consecutive prime divisors p_i and p_j of x such that $a \equiv a' \bmod p_i{}^{\alpha_i}$ and $a \not\equiv a' \bmod p_j{}^{\alpha_j}$. But then we obtain a contradiction in the same way by observing that $a \equiv a' \bmod p_i{}^{\alpha_i}$ implies that there is a $\gamma < p_i{}^{\alpha_i}$ such that $a \equiv \gamma \bmod p_i{}^{\alpha_i}$ and $a' \equiv \gamma \bmod p_i{}^{\alpha_i}$ with as a result that $a \equiv \gamma' + \gamma \equiv a' \bmod p_j{}^{\alpha_j}$ for γ such that $v_y(p_j\text{-}1) = \gamma$ contradicting our assumption. Note that we do not automatically get: $\forall x, p$ "prime" $\exists \beta\, A(x, p, \beta)$. The reason for this is obviously hidden in the fact that we can not straightforwardly prove (in $I\Delta_0$) that the witness that we use in the definition of $A(x, p, \beta)$ is sufficiently small. That is precisely what we have to prove by induction.
ii. Let x be of the form q^n for q prime and let p be prime. If $p \geq q$, then 0 is the unique witness of the iterated sum of exponents of exact powers of p that divide q-1. This is

easily proved by observing that there is only one prime divisor in x, namely q, and that p^0 is the only power of p dividing q-1. In this case $A(x, p, 0)$ will hold, so we have:
$A(x, p, z)$ holds iff $v_p(q\text{-}1) = z$.

If $p < x$, then there is something to prove. If $A(x, p, z)$ holds, there will be an $a < x$, such that $a \equiv \gamma \bmod p_i^{\alpha_i}$ with $v_p(q\text{-}1) = \gamma$ and $p_i^{\alpha_i}$ being the greatest power of the greatest prime number p_i that divides x, that is, x itself. Since the least and the greatest prime divisors of x coincide, we can also conclude that $z \equiv \gamma \bmod x$ for $v_p(q\text{-}1) = \gamma$. But we also have: $\gamma < x$, so $v_p(q\text{-}1) = z$. Conversely, if $v_p(q\text{-}1) = z$ holds, then take z to be the desired witness ($z \equiv z \bmod x$ holds, as well as $z < x$).

iii. Let x be of the form $p_m{}^n.r$ where p_m is the greatest prime number dividing x and $gcd(p_m, r) = 1$, let $p < p_m$ be a prime number and γ, δ be such that $A(r, p, \gamma)$ as well as $A(p_m{}^n, p, \delta)$ hold. By i it is sufficient to show: $A(x, p, \gamma + \delta)$. This is the point where we have to use Legendre's theorem, or rather the part of it that $I\Delta_0$ proves. Heuristically one can remark that since we do not know exactly what $I\Delta_0$ proves about the division of the primes, we have to take into account the possibility that $I\Delta_0$ encounters a very dense sequence of prime numbers while storing the iterated sum of exponents of greatest powers of p that divide the various predecessors of these prime numbers. That could cause some trouble as to the trustworthiness of our construction with the Chinese Remainder Theorem. Surprisingly in a way, the bound that Legendre's theorem offers is just accurate enough, as we shall now see. We will show by induction on the exact powers of the primes that divide a number x, that we actually have:

$$\forall p \text{ "prime"}, p_m \text{ "greatest prime number dividing } x\text{"} \; \exists \beta \leq \frac{p_m - \#_p p_m}{p-1} \, A(x, p, \beta).$$

To see this, fix p prime. If x is of the form q^n for q prime, then β is the exponent of the exact power of p that divides q - 1. But, by Proposition 2.2 (iii), we have:

$$(p - 1).\ v_p(p_m - 1) \leq p_m - \#_p(p_m).$$

On the other hand, if x is of the form $p_m{}^n.r$ where p_m is the greatest prime number dividing x and $gcd(p_m, r) = 1$, and p_r is the greatest prime number that divides r, then by induction hypothesis we can assume that if $A(r, p, \gamma)$ holds, then $\gamma \leq \frac{p_r - \#_p p_r}{p-1}$. Suppose that $p < p_r$. Since $A(r, p, \gamma)$ holds, there is a witness, say a, that produces the number γ and it is sufficient to extend a with the exponent of p in p_m - 1, which is $v_p(p_m - 1)$. In other words, if $s < p_m{}^n$ and $t < r$ are given by means of Bézout's theorem in such a way that $t.p_m{}^n - s.r = 1$, then we let a' be the smallest number such that:

$$a' \equiv (a.p_m{}^n.t + (\gamma + v_p(p_m - 1)).s.r) \bmod x.$$

Now a' has the same residues as a for the prime divisors of r. It is easily verified that a' is the witness for the iterated sum of exponents of the greatest powers of p that divide the numbers of the form q - 1 where q divides x. For that reason and the fact that we now have: $a' \equiv \gamma + v_p(p_m - 1) \bmod p_m{}^n$, we can infer $A(x, p, \gamma + v_p(p_m - 1))$ once we know that $\gamma + v_p(p_m - 1)$ is smaller than $p_m{}^n$.

By Proposition 2.2, we can now conclude (if indeed $p_m > p_r + 1$):

$$\begin{aligned} \gamma + v_p(p_m - 1) &\leq \frac{p_r - \#_p p_r}{p-1} + v_p(p_m - 1) \\ &= \frac{p_r - \#_p p_r + (p-1).v_p(p_m - 1)}{p-1} \\ &\leq \frac{(p_m - 1) - \#_p(p_m - 1)}{p-1} \text{ (by ii in Proposition 2.2)} \\ &\leq \frac{p_m - \#_p p_m}{p-1} \text{ (by i in Proposition 2.2).} \end{aligned}$$

Otherwise, if $p_m = p_r + 1$, then we are in the situation where $p = 2 = p_r$ contradicting our assumption that $p < p_r$.

On the other hand, if p is greater, that is, if $p_r \leq p < p_m$ is the case, then it is easily verified that p will not divide any number of the form $q - 1$, where q is a prime divisor of r. In that situation, $A(p_m^n, p, \beta)$ will hold if and only if $A(x, p, \beta)$ holds, from which the result follows directly.

Now that this bound has been established, we can proceed with the proof. If $A(r, p, \gamma)$ as well as $A(p_m^n, p, \delta)$ hold, then we can find a witness of the iterated sum of exponents of p that divide the numbers $q - 1$ for q the prime divisors of x, in just the same fashion as above. Checking the fact that $A(x, p, \gamma + \delta)$ holds is easily executed, since we can safely assume: $\gamma + \delta \leq \frac{p_m - \#_p p_m}{p-1} \leq p_m^n$.

iv. Let x be of the form q^n for q prime. It is clear that we are in a situation that $Z(z_x, x)$ holds if and only if $\forall p, \beta \leq z_x[v_p(z_x) = \beta \leftrightarrow (A(x, p, \beta)]$, which is equivalent (by ii) with $\forall p, \beta \leq z_x[v_p(z_x) = \beta \leftrightarrow v_p(q-1) = \beta\ ]$. Now it is evident that the number q-1 is the unique number that satisfies the requirement.

v. In order to get this lemma, we will first prove a reduced statement: for any x, if p_m is the greatest prime number dividing x and p_m^n is the exact power of p_m dividing x, then $Z(z_x, x)$ holds iff $z_x = (p_m - 1).z_r$ for r such that $p_m^n.r = x$ and z_r such that $Z(z_r, r)$. This is showed in the following way. By inspecting the definitions, it is provable in $I\Delta_0$ that for every $p \leq z_x$ prime, the number β for which $v_p(z_x) = \beta$ holds is exactly the number $\gamma + \delta$ such that $A(r, p, \gamma)$ and $A(p_m^n, p, \delta)$ hold (by iii). But now, by comparing the exponents (using proposition 2.9), this implies: $z_x = (p_m - 1).z_r$.

To get the general case let the conditions be as stated. If $t = 1$, there is nothing to prove. Therefore suppose that neither of s and t is equal 1. Let p_m^n be the exact power of the greatest prime number p_m that divides x occurring in the factorisation of x. Without loss of generality we can assume that $s = p_m^n.r$, because s and t can not have the factor p_m in common as they are relatively prime. By the preceding argument we have that $Z(z_x, x)$ holds if and only if $z_x = (p_m - 1).z_{r.t}$, for $z_{r.t}$ such that $Z(z_{r.t}, r.t)$ holds. By induction we can now conclude: $z_{r.t} = z_r.z_t$ for z_r, z_t such that $Z(z_r, r)$ and $Z(z_t, t)$ hold respectively. But then we also know that $z_x = (p_m - 1).z_r.z_t$ and $Z((p_m - 1).z_r, s)$, so we get the result: $z_x = z_s.z_t$.

Notice that the fact that the predicate $Z(x, y)$ defines a function follows from the observation that if $Z(z_x, x)$ holds, then y is uniquely determined by its decomposition in prime factors.

We are now in a position to prove that $\varphi(x, y)$ behaves as we claimed in the initial theorem of this chapter. This can easily be inferred from the proposition below.

PROPOSITION 2.10. $I\Delta_0$ proves the following facts:
i. "$\varphi(1, 1)$",
ii. "if x is of the form q^n for q prime, $n \neq 0$, then $\varphi(x, (q - 1).q^{n-1})$",
iii. "if x is of the form $p_m{}^n.r$ where p_m is the greatest prime number dividing x and $p_m{}^n$ is the greatest power of p_m dividing x and if $gcd(p_m, r) = 1$ and $\varphi(r, u)$, then $\varphi(x, u. (p_m - 1).p_m{}^{n-1})$",
iv. "if $x = s.t$ and $gcd(s, t) = 1$ and $\varphi(s, u)$ and $\varphi(t, v)$, then $\varphi(x, u.v)$",
v. "$\varphi(x, y)$ defines a total function",
vi. "if p is a prime divisor of x and r is such that $r.p = x$, then, if not $p^2|x$ and $\varphi(r, s)$ holds, this will imply $\varphi(m, (p-1).s)$ and if $p^2|m$, then $\varphi(m, p.s)$".

PROOF. Reason in $I\Delta_0$.
i. Immediate from $Z(1, 1)$ and $Y(1, 1)$.
ii. Let x be of the form q^n, $n \neq 0$. By definition we have $Y(q^{n-1}, x)$ and by iv above we have $Z(q - 1, x)$. Therefore also by the definition of $\varphi(x, y)$: $\varphi(x, (q - 1).q^{n-1}))$.
iii. Let the conditions be as stated. If $\varphi(r, u)$ holds, then apparently there are numbers y_r and z_r such that $Y(y_r, r)$ and $Z(z_r, r)$ which, if multiplied with each other, yield u. Because $p_m{}^n$ is relatively prime to r, we have $Z((p_m - 1).z_r, x)$ and also, for more trivial reasons: $Y(p_m{}^{n-1}.y_r, x)$, thus $\varphi(x, u. (p_m - 1).p_m{}^{n-1})$.
iv. If $x = s.t$ and $gcd(s, t) = 1$ and $\varphi(s, u)$ and $\varphi(t, v)$ hold, then apparently there are y_t, z_t, y_s, z_s such that $Y(y_t, t)$, $Z(z_t, t)$, $Y(y_s, s)$, $Z(z_s, s)$ all hold with $z_s.y_s = u$ and $z_t.y_t = v$. As a consequence of iv above, we have $Z(z_s.z_t, s.t)$ and also $Y(y_s.y_t, s.t)$ and therefore also $\varphi(x, u.v)$.
v. By plain Δ_0-induction, using i, ii and iii above (note that we can prove the expression: $\forall x \exists y \leq x\ \varphi(x, y)$).
vi. Immediate from ii above.

From the last proposition we can easily infer i, ii, and iii of our initial theorem.

§3. Comment. In a certain sense $I\Delta_0$ may not know that the formula about which it proves the recursion equations cited in the proposition above describes the cardinality of a set of the form $\{m<n \mid \gcd(n, m) = 1\}$. We will briefly discuss this topic.

Given Euler's φ-function, (the result in §2 justifies our use of the functional expression for φ in $I\Delta_0$) the question whether it counts what it should count can be made explicit by reformulating it in the following way: can we construct a Δ_0-function $g(a, x)$ such that it is provable in $I\Delta_0$ that this definition satisfies the recursion equations that accompany the counting procedure of numbers less than or equal to x and having greatest common divisor 1 with a? So, we are asking for a Δ_0-function g that satisfies the following requirement:

$$I\Delta_0 \vdash \forall a, x\ (\ \gcd(a, x+1) = 1 \wedge x+1 \leq a \leftrightarrow g(a, x+1) = g(a, x)+1).$$

If this can be done, then do we necessarily have:

$$I\Delta_0 \vdash \forall a\ g(a, a) = \varphi(a)?$$

Evidently, it is possible to find a formula that works for (powers of) prime numbers, namely, by means of a construction similar to the one in the theorem of Legendre that we used to obtain our definition of Euler's φ-function, but that does not at all solve the general problem.

Another version of this problem may be that, with Euler's φ-function in hand, we can investigate whether we can prove in $I\Delta_0$ some theorems that are directly connected with this function. For instance, we may ask whether we can attach any meaning to Gauss' formula, that is, to the statement:

$$\text{for all } n \in \mathbb{N}\text{: } n = \sum_{d \mid n} \varphi(d).$$

In order to find the meaning, if any, of this statement for a theory like $I\Delta_0$, we should first ask whether the following function can be formalised by means of a Δ_0-formula:

$$f(a, x) := \sum_{d \mid a \ \&\ d \leq x} \varphi(d).$$

It is clear that this function counts elements z that satisfy the following Δ_0-formula:

$$A(a, x, z) := \exists d \leq x\ [d \mid a \wedge \exists y < d\ (\gcd(y, d) = 1 \wedge d.z = a.y)].$$

Furthermore, by formalisation we mean to find a Δ_0-formula $f(a, x)$ such that the recursion equation that goes with it is indeed proved by $I\Delta_0$, so we should have:

$$I\Delta_0 \vdash \forall a, x(x+1 \leq a \rightarrow (x+1 \mid a \rightarrow (f(a, x+1) = f(a, x) + \varphi(x+1)) \wedge (\neg x+1 \mid a \rightarrow f(a, x+1) = f(a, x))).$$

It is doubtful whether this function can indeed be described by means of a Δ_0-formula.

The remarks about Gauss' formula may be put in a more general perspective if confronted with questions about the behaviour of summations that are defined by means of the Möbius function inside a theory like $I\Delta_0$.

The Möbius function itself is rather easily definable. It can be done by means of the Chinese Remainder Theorem if we choose some representation of the set {0, 1, -1}. If

we consider the way in which Euler's φ-function is computed by means of the Möbius function, that is by means of the formula

$$\varphi(n) := \sum_{d|n} d.\mu(\tfrac{n}{d}),$$

then we are led to ask whether the following function (which may take its values in $\mathbb{Z}$, but that is a minor complication easily solved with the use of a pairing function) is Δ_0-definable:

$$\psi(m, n) := \begin{cases} 0 & \text{for } m \nmid n, \\ \sum_{d|m} d.\mu(\tfrac{n}{d}) & \text{for } m|n. \end{cases}$$

The last summation describes the way in which the φ-function is computed by means of the principle of inclusion-exclusion, so we should also ask whether we necessarily obtain the obvious: $\psi(n, n) = \varphi(n)$. But now we find that this approach does not learn us much about Möbius inversion because the function $\psi(x, y)$ is indeed trivially formalisable by means of a definition of Euler's φ-function, by putting:

$$\psi(m, n) := \begin{cases} 0 & \text{for } m \nmid n, \\ \frac{\varphi(n)}{\varphi(n/m)}.\mu(\tfrac{n}{m}) & \text{for } m|n. \end{cases}$$

This definition represents the function (at least in $\mathbb{N}$) by means of a Δ_0-formula and it may be verified (by a very lengthy inductive argument) that $I\Delta_0$ proves the recursion equations that articulate the properties of $\psi(x, y)$. It seems therefore that the problems only arise once we combine two different orderings.

The following, very simple, example may help to illustrate in a different way why $I\Delta_0$ may not know what its version of Euler's φ-function is counting.

Fix a natural number $n \geq 2$. Let, for some number $x \geq 2$, m be the number $x^n - 1$. Since x has no divisor in common with m except 1, we can consider x as an element of $(\mathbb{Z}/m\mathbb{Z})^*$. Therefore, the order of x, say e, has to be a divisor of n. So, we have that $n = k.e$, for some k. But, if $k \neq 1$, then evidently $x^e - 1 < x^n - 1 = m$, which implies that m can not be a divisor of $x^e - 1$. If we continue to reason about $(\mathbb{Z}/m\mathbb{Z})^*$, we can state that this multiplicative group has an element of order n. As it is a fundamental fact of elementary group theory that the order of any element divides the order of the group itself, we may

conclude that n is a divisor of the cardinality of $(\mathbb{Z}/m\mathbb{Z})^*$ that is, of the cardinality of the set $\{i<m \mid \gcd(i, m) = 1\}$. Thus, if we use Euler's φ-function, we obtain the proposition: $n|\varphi(x^n - 1)$. This is a statement that we can express in the language of $I\Delta_0$ and therefore it is natural to ask the following: given a model M of $I\Delta_0$, what is the set of elements n of M such that $M \models$ "$\forall x \geq 2\ n|\varphi(x^n - 1)$"?

The least that we know is that the standard numbers n=2, 3, 4 are in this set. We find the proofs of these facts in the propositions that list what $I\Delta_0$ can prove about the behaviour of quadratic residues for prime numbers. These proofs can be found in Smith [4]. From these proofs it is quite evident that the kind of reasoning that $I\Delta_0$ employs has very little in common with the proof above which used elementary group theory.

We remark that the proof for the expression x^n-1 in case n is a standard prime can easily be done with the help of the equipartition principle (cf. Berarducci & Intrigila [1]). In that case, we can reason as follows: given a number ξ, let p be a prime number with the property that $p|\xi^n$-1 and let an equivalence relation $R(x, y)$ be defined on the elements of the multiplicative group $\mathbb{F}_p^*$ by means of the following definition:

$R(x, y)$ iff $\exists m\ 1 \leq m \leq n\ a \equiv b.\xi^m \bmod p$.

Every equivalence class will now be of the form $\{a,\ldots, a.\xi^{n-1}\}$ (all elements mod p) and will contain exactly n elements because ξ^m can not be congruent to $\xi^{m'}$ modulo p for numbers m, m' such that $1 \leq m, m' \leq n$ if n is a fixed standard prime number. The equipartition principle will tell us now that n must be a divisor of the cardinality of $\mathbb{F}_p^*$, that is, of the number p-1 and we are done.

As to the case of $n = 5$ we can show that if a prime number p divides $\xi^5 - 1$ for some $\xi \neq 1$, then at least 5 will be a quadratic residue for p, so we get $p \equiv \pm 1 \pmod 5$ (cf. Smith [4]), but that is where the argument comes to a standstill. What we have to do next, is to show that no prime number $p \equiv -1 \pmod 5$ can divide $\xi^4 + \xi^3 + \xi^2 + \xi + 1$. However, it is still not excluded that we can get the result for $n = 5$ by meticulously adapting the same technique as the one used to get the results for quadratic reciprocity.

References.

[1] Berarducci, A. & Intrigila, B., Combinatorial principles in elementary number theory, *Annals of Pure and Applied Logic*, Vol. 55, Number 1, 1991.

[2] Hájek, P. & Pudlák, P., *Metamathematics of First-Order Arithmetic*, Springer-Verlag, 1993.

[3] Paris, J. B. & Wilkie, A. J., Counting Δ_0 sets, *Fund. Math.* Vol. 127, 1987, pp. 67-76.

[4] Smith, S. T., Quadratic Residues and $x^3 + y^3 = z^3$ in Models of IE_1 and IE_2, *Notre Dame Journal of Formal Logic*, Vol. 34, Number 3, 1993.

[5] Smoryński, C., *Logical Number Theory I*, Springer Verlag, 1991.