Return to website: https://www.peterbraun.com.au

Dirichlet's theorem for square free forms
by
Peter Braun

Introduction

The 'uniqueness' of factorisation of natural numbers as a product of prime powers allows the notion of number form to be defined. That is, the essential prime structure allows an equivalence relation to be defined.

For example, 3 is an instance of the form p where p is prime and the set of numbers of this form we denote by [p].

[2.3] = [pq] where p and q are distinct primes and [4] = [p^2] and so on.

Forms [$p_1p_2....p_r$] where p_1, p_2, p_r represent the square free numbers for r= 1,2,3… .

We note that a number K is represented by the progression an+b if and only if

$K \equiv b \bmod a$.

Let (a, b) = 1 and aN+b = {an+b : n∊ N} where N denotes the natural numbers.

Proposition

For any fixed r, r ≥ 1, aN+b contains unbounded instances of numbers belonging to the form [$p_1p_2....p_r$].

Proof

The theorem is obvious in the case a = 1.

The hard work has been done in the proof of the theorem for prime numbers.

We consider the congruence -

$x\, a_2...a_r \equiv b \bmod a$ where $a =(q_1)^{\alpha_1}(q_2)^{\alpha_2}...(q_s)^{\alpha_s}$ and $a_2 ....a_r$ are any given numbers co prime to a and b and we assume the q_i are distinct primes.

We know from the Chinese remainder theorem that there is a solution $x = a_1$ to this congruence and $(a, a_1) = 1$.

Then note that $(a_1+ \theta_1a)(a_2 + \theta_2a)....(a_r + \theta_ra) \equiv b \bmod a =(q_1)^{\alpha_1}(q_2)^{\alpha_2}...(q_s)^{\alpha_s}$ (for any $\theta_1, \theta_2... \theta_r$.

Select values for these variables so that $a_1+ \theta_1a$, $a_2 + \theta_2a... a_r + \theta_ra$ are distinct prime numbers.

For these values we have $(a_1+ \theta_1a)(a_2 + \theta_2a)....(a_r + \theta_ra) \equiv b \bmod a$.

Hence the progression aN+b takes the value $(a_1+ \theta_1a)(a_2 + \theta_2a)....(a_r + \theta_ra)$ and this number belongs to the form [$p_1p_2.... p_r$] where $p_1, p_2.... p_r$ are distinct primes.

It is clear that this process allows unbounded numbers from this form in the function values of the progression.

In an earlier draft the author stated and proved erroneously that with (a,b) = 1, aN+b supports numbers of all forms.

It was pointed by D. Dona [1] that such a generalisation is false.

For example: 4N+3 cannot represent any elements of [n^2] since $n^2 \equiv 3 \bmod 4$ is impossible.

Dona's defines forms [n] as Dirichlet forms if and only if all arithmetic progressions aN+b with (a,b) =1 include unbounded numbers of the form.

He conjectured and proved that [$p_1^{a_1}p_2^{a_2}....p_n^{a_n}$] is a Dirichlet form if and only if $(a_1,a_2, ...a_n) = 1$. We follow his approach for the sufficient part of this condition but include a simplified proof for the necessity of the condition.

November 2012

We note that if $aN+b$ represents a form at all then it represents an unbounded number of the form.

Indeed, $aN+b = X$ iff $X\equiv a \bmod b$.

The form $[p_1^{a_1}p_2^{a_2}\ldots\, p_n^{a_n}]$ is represented by $aN+b$ iff there exist primes $p_1, p_2, \ldots, p_n$ such that $p_1^{a_1}p_2^{a_2}\ldots\, p_n^{a_n} \equiv b \bmod a$.

If we have $p_1^{a_1}p_2^{a_2}\ldots\, p_n^{a_n} \equiv b \bmod a$, then
$(p_1+\theta_1 a)^{a_1}(p_2+ \theta_2 a)^{a_2}\ldots\ldots(p_n+ \theta_n a)^{a_n} \equiv b \bmod a$ for arbitrary numbers $\theta_1, \theta_2, \ldots, \theta_n$.
We may choose unbounded collections $\theta_1, \theta_2, \ldots, \theta_n$ such that each of

$(p_1+\theta_1 a), (p_2+ \theta_2 a), \ldots\ldots, (p_n+ \theta_n a)$ is prime.

For these choices $aN+b$ represents $(p_1+\theta_1 a)^{a_1}(p_2+ \theta_2 a)^{a_2}\ldots\ldots(p_n+ \theta_n a)^{a_n}$.

Proof of Dona's Theorem

Necessary

Suppose $(a_1,a_2, \ldots,a_n) = d$ with $d > 1$.

Let $(d, r_0) =1$ and suppose $d^2N_0+ r_0 = n_0^d$ for any fixed form $[n_0]$.

Let $n_0 = g_0 d + h_0$. We note $(d, h_0) = 1$ and so h_0^d is one of the $\varphi(d)$ numbers co-prime to d.

Noting $n_0^d = (g_0 d + h_0)^d = \lambda_0 d^2 + h_0^d$, the proof follows from the observation that at most $\varphi(d)$ of $d^2N+d_1, d^2N+d_2, \ldots\ldots d^2N +d_{\varphi(d^2)}$ represent $[n_0^d]$ and $\varphi(d) < \varphi(d^2)$.

Sufficient

Let $(a, b) =1$ and suppose $(a_1, a_2 \ldots a_n) =1$.

Then there exists integers $\lambda_1, \lambda_2, \ldots, \lambda_n$ such that $\lambda_1 a_1+ \lambda_2 a_2+ \ldots \lambda_n a_n = 1$.

Then $(b^{\lambda_1})^{a_1}(b^{\lambda_2})^{a_2}\ldots(b^{\lambda_n})^{a_n} \equiv b \bmod a$.

If an index λ_i is negative we may substitute $\lambda_i + K\varphi(a) > 0$ so we may assume without loss of generality that $\lambda_1, \lambda_2\ldots, \lambda_n$ are natural numbers.

Then there are natural numbers $x_1, x_2, \ldots, x_n$ such that $(x_1)^{a_1}(x_2)^{a_2} \ldots(x_n)^{a_n} \equiv b \bmod a$.

Since there is a solution there are an unbounded number of solutions.

References

D. Dona University of Turin – email correspondence.

November 2012