MATH. SCAND. 114 (2014), 161–184

# ON FIXED DIVISORS OF FORMS IN MANY VARIABLES, I

A. SCHINZEL

(In memory of Trygve Nagell)

## Abstract

Let $D_{d,r}$ be the maximal fixed divisor of a primitive form of degree $d$ in $r$ variables over $\mathsf{Z}$. A formula is given for $D_{d,2}$ and estimates for $D_{d,r}$ for $r > 2$. As a consequence, a question of Nagell raised in 1919 is completely answered.

Let $K$ be a finite extension of $\mathsf{Q}$ and for $f \in K[x_1, \dots, x_r]$ let $C(f)$ and $D(f)$ be the highest common ideal factor of the coefficients of $f$ and of the values of $f$ for $\mathbf{x} \in \mathsf{Z}^r$, respectively. Polynomials $f$ with $C(f) = 1$ are called primitive. For a prime ideal $\mathfrak{p}$ and an ideal $\mathfrak{a}$ of $K$, let $\operatorname{ord}_{\mathfrak{p}} \mathfrak{a}$ be the exponent with which $\mathfrak{p}$ occurs in the factorization of $\mathfrak{a}$. T. Nagell has proved ([5], p. 16) that for every $f \in \mathsf{Z}[x_1, \dots, x_r]$ of degree $d$

$$D(f) \mid d!C(f). \tag{1}$$

This result is implicit in [4]. An easy generalization is contained in

THEOREM 1. *For every finite extension $K$ of $\mathsf{Q}$ and for every $f \in K[x_1, \dots, x_r]$ of degree $d$* (1) *holds.*

Put

$$S_{d,r} = \{F \in \mathsf{Z}[x_1, \dots, x_r], \text{ of degree } d, \text{ homogeneous and primitive}\},$$
$$S^0_{d,r} = \{F \in S_{d,r}, \text{ splitting over } \mathsf{C}\},$$
$$S^1_{d,r} = \{F \in S_{d,r}, \text{ splitting over } \mathsf{Z}\}.$$

It follows from (1) that the following definitions are correct:

$$D_{d,r} = \max_{f \in S_{d,r}} D(f), \qquad D^1_{d,r} = \max_{f \in S^1_{d,r}} D(f).$$

For $K = \mathsf{Q}$, $D(F)$ is identified with its positive generator. We shall prove

Received 14 October 2011, in final form 20 August 2012.

THEOREM 2. *For all* $F \in S^0_{d,r}$ *and for all primes* $p$

$$\operatorname{ord}_p D(F) \le \operatorname{ord}_p\left(\left(p\left\lfloor \frac{(p^{r-1}-1)d}{p^r-1}\right\rfloor\right)!\right).$$

THEOREM 3. *For all positive integers* $d$ *and* $r > 1$ *and for all primes* $p$

$$\operatorname{ord}_p D^1_{d,2} \ge \operatorname{ord}_p\left(\left(p\left\lfloor \frac{d}{p+1}\right\rfloor\right)!\right),$$

$$\operatorname{ord}_p D^1_{d,r} \ge (p^{r-1}-1)q^{r-1}\operatorname{ord}_p((pq)!) + \operatorname{ord}_p\left(\left(p\left\lfloor \frac{d-(p^r-1)q^r}{p+1}\right\rfloor\right)!\right),$$

*where* $q = \left\lfloor \sqrt[r]{\frac{d}{p^r-1}} \right\rfloor$.

COROLLARY 1. *For all positive integers* $d$ *and for all primes* $p$

$$\operatorname{ord}_p D_{d,2} = \operatorname{ord}_p\left(\left(p\left\lfloor \frac{d}{p+1}\right\rfloor\right)!\right) = \operatorname{ord}_p D^1_{d,2}.$$

COROLLARY 2. *The least integer* $d$, *say* $d_2(n)$, *such that* $n! \mid D_{d,2}$ *is* 4 *for* $n = 3$ *and* $3\left\lfloor \frac{n}{2}\right\rfloor$, *otherwise.*

The corollary answers a question asked by Nagell [5]. He has proved that $d_2(2) = 3$, $d_2(3) = 4$, $d_2(4) = d_2(5) = 4$, $d_2(n) \le 2n-1$. The last result has been anticipated by Hermite (see [2], p. 266).

COROLLARY 3. *For all integers* $d \ge 3$ *and* $r \ge 2$ *and for all primes* $p < d$

$$\operatorname{ord}_p D^1_{d,r} = d\left(\frac{1}{p-1} - \frac{1}{p^r-1}\right) + d^{\frac{r-1}{r}} O\left(\frac{r}{p} + \frac{\log d}{r\log p} + 1\right),$$

*where the constant in the* $O$*-symbol is absolute and* $d^{\frac{r-1}{r}}$ *can be omitted for* $r = 2$.

COROLLARY 4. *For all integers* $r \ge 2$

$$\log D_{d,r} = d\log d + O(d)$$

*uniformly in* $r$.

THEOREM 4.

(i) *For all positive integers* $d$ *and* $r$

$$D_{d,r} \mid (d-1)!$$

(ii) *For all integers* $d \geq 4$, $r_d = d - \operatorname{ord}_2\big(\big(2\lfloor \frac{d}{3} \rfloor\big)!\big) - 1$ *and* $r \geq r_d$,

$$D_{d,r} = D_{d,r_d}.$$

COROLLARY 5. *For all positive integers* $d \leq 6$ *and* $r \geq 2$

$$D_{d,r} = D_{d,2}.$$

COROLLARY 6. $D^1_{9,3} = D^1_{9,2}$.

Corollary 1 suggests the following

CONJECTURE. *For all positive integers* $d$ *and* $r$

$$D_{d,r} = D^1_{d,r}.$$

This is true for $d < 9$ and each $r$, see Remark after the proof of Corollary 5.

THEOREM 5. *Let* $d_r(n)$ *be the least integer* $d$ *such that* $n! \mid D_{d,r}$. *Then for all* $r$ *the limit* $l_r = \lim_{r\to\infty} \frac{d_r(n)}{n}$ *exists and satisfies* $l_r \leq \frac{2^r-1}{2^r-2}$. *If Conjecture is true we have equality.*

THEOREM 6. *For all positive integers* $d \geq 3^4 \cdot 2^3 = 648$ *and* $r = \lfloor \frac{-1+\sqrt{8d+1}}{2} \rfloor$

$$D_{d,r} \equiv 0 \mod \lceil d - 3(2d)^{3/4} \rceil !.$$

COROLLARY 7. *For* $r \geq \lfloor \frac{-1+\sqrt{8d+1}}{2} \rfloor$ *we have*

$$\log D_{d,r} = d \log d - d + O(d^{3/4} \log d)$$

*uniformly in* $r$.

PROOF OF THEOREM 1. Since $x^n$ is a linear combination of $\binom{x}{j}$ $(j = 0, \ldots, n)$ with integral coefficients, it follows that

$$f = \sum_{\mathbf{i} \in \mathbf{I}_d} \alpha_{\mathbf{i}} \binom{x_1}{i_1} \ldots \binom{x_r}{i_r}, \tag{2}$$

where $\mathbf{I}_d = \{\, \mathbf{i} = [i_1, \ldots, i_r] : i_1 + \cdots + i_r \leq d \,\}$, $\alpha_{\mathbf{i}} \in K$. We shall show by induction on $k$ that

$$D(f) \mid \alpha_{\mathbf{i}} \qquad \text{for} \quad \mathbf{i} \in \mathbf{I}_k. \tag{3}$$

Since $\alpha_0 = f(\mathbf{0})$, (3) holds for $k = 0$. Assume that it holds for $k$ and let $j_1 + \dots + j_r = k + 1$. By the inductive assumption

$$D(f) \Big| \sum_{\mathbf{i} \in \mathbf{I}_k} \alpha_{\mathbf{i}} \binom{x_1}{i_1} \dots \binom{x_r}{i_r} \qquad \text{for all} \quad \mathbf{x} \in \mathsf{Z}^r,$$

hence, by (2),

$$D(f) \Big| \sum_{\mathbf{i} \in \mathbf{I}_d \setminus \mathbf{I}_k} \alpha_{\mathbf{i}} \binom{x_1}{i_1} \dots \binom{x_r}{i_r} \qquad \text{for all} \quad \mathbf{x} \in \mathsf{Z}^r. \tag{4}$$

Since for $\mathbf{i} \in \mathbf{I}_d \setminus \mathbf{I}_k$ we have $i_1 + \dots + i_r \geq k + 1 = j_1 + \dots + j_r$ we obtain either $i_s = j_s$ for all $s \leq r$ or $i_s > j_s$ for at least one $s \leq r$. Therefore,

$$\sum_{\mathbf{i} \in \mathbf{I}_d \setminus \mathbf{I}_k} \alpha_{\mathbf{i}} \binom{j_1}{i_1} \dots \binom{j_r}{i_r} = \alpha_{\mathbf{j}}$$

and, by (4), $D(f) \mid \alpha_{\mathbf{j}}$, which completes the inductive proof of (3). Now,

$$D(f) \operatorname*{g.c.d.}_{\mathbf{i} \in \mathbf{I}_d} \alpha_{\mathbf{i}} \Big| \operatorname*{g.c.d.}_{\mathbf{i} \in \mathbf{I}_d} \binom{d}{i_1, \dots, i_r} \alpha_{\mathbf{i}} \Big| d! \operatorname*{g.c.d.}_{\mathbf{i} \in \mathbf{I}_d} \frac{\alpha_{\mathbf{i}}}{i_1! \dots i_r!} \Big| d! C(f).$$

REMARK. In the same way one can prove that all values of a polynomial $f \in K[x_1, \dots x_r]$ at $\mathbf{x} \in \mathsf{Z}^r$ belong to an ideal $\mathfrak{a}$ of $K$, if and only if $f = \sum_{i \in \mathbf{I}} a_{\mathbf{i}} \binom{x_1}{i_1} \dots \binom{x_r}{i_r}$, where $a_{\mathbf{i}} \in \mathfrak{a}$ for all $i \in \mathbf{I}$.

For the proof of Theorem 2 we need two lemmas.

LEMMA 1. *For every prime $p$ and positive integer $n$*

$$\operatorname{ord}_p(n!) = \frac{n - s_p(n)}{p - 1},$$

*where $s_p(n)$ is the sum of digits of $n$ in the base $p$.*

PROOF. See [1], pp. 54–55.

LEMMA 2. *For every finite field $\mathsf{F}_q$, where $q = p^f$ ($p$ prime) and every vector $\mathbf{v} \in \mathsf{F}_q^r \setminus \{\mathbf{0}\}$ there exist at most $p^{r-1} - 1$ vectors $\mathbf{x} \in \mathsf{F}_p^r \setminus \{\mathbf{0}\}$ such that*

$$\mathbf{v}\mathbf{x} = 0. \tag{5}$$

PROOF. Let $w_1, \dots, w_f$ be a basis of $\mathsf{F}_q$ over $\mathsf{F}_p$ and let $\mathbf{v} = \sum_{i=1}^{f} \mathbf{v}_i w_i$, $\mathbf{v}_i \in \mathsf{F}_p^r$. Since $\mathbf{v} \neq \mathbf{0}$ we have $\mathbf{v}_j \neq \mathbf{0}$ for at least one $j \leq f$. Moreover, the

equation (5) gives $\mathbf{v}_i\mathbf{x} = 0$ for all $i \le f$, hence the number in question does not exceed the number of non-zero solutions of $\mathbf{v}_j\mathbf{x} = 0$, which is $p^{r-1} - 1$.

PROOF OF THEOREM 2. Let $K$ be a splitting field of $F$ and

$$F = \prod_{i=1}^{d} L_i,$$

where $L_i \in K[x_1, \dots, x_r]$ are linear forms. Let $\mathfrak{p}$ be a prime ideal of $K$ and let $\pi$ be an element of $K$ such that $\operatorname{ord}_{\mathfrak{p}} \pi = 1$. Since $C(F) = 1$, multiplying $L_i$ by a suitable power of $\pi$ we may achieve

$$\operatorname{ord}_{\mathfrak{p}} C(L_i) = 0 \qquad (1 \le i \le d). \tag{6}$$

Let norm $\mathfrak{p} = q$ and for $\mathbf{v} \in \mathsf{F}_q^r \setminus \{\mathbf{0}\}$

$$N_{\mathbf{v}} = \{i \le d : \ L_i \equiv v_1x_1 + \cdots + v_rx_r \bmod \mathfrak{p}\}.$$

By Lemma 2

$$\sum_{\mathbf{x}\in\mathsf{F}_p^r\setminus\{\mathbf{0}\}} \sum_{\substack{\mathbf{v}\in\mathsf{F}_q^r\setminus\{\mathbf{0}\}\\ \mathbf{vx}=0}} |N_{\mathbf{v}}| = \sum_{\mathbf{v}\in\mathsf{F}_p^r\setminus\{\mathbf{0}\}} |N_{\mathbf{v}}| \sum_{\substack{\mathbf{x}\in\mathsf{F}_p^r\setminus\{\mathbf{0}\}\\ \mathbf{vx}=0}} 1$$
$$\le (p^{r-1} - 1) \sum_{\mathbf{v}\in\mathsf{F}_q^r\setminus\{\mathbf{0}\}} |N_{\mathbf{v}}| = (p^{r-1} - 1)d.$$

It follows that there exists $\mathbf{x}^0 \in \mathsf{Z}^r$, $\mathbf{x}^0 \not\equiv \mathbf{0} \bmod \mathfrak{p}$ such that denoting by $\overline{\mathbf{x}}^0$ the residue class of $\mathbf{x}^0 \bmod p$ we have

$$s(\mathbf{x}^0) := \sum_{\substack{\mathbf{v}\in\mathsf{F}_q^r\setminus\{\mathbf{0}\}\\ \mathbf{v}\overline{\mathbf{x}}^0=0}} |N_{\mathbf{v}}| \le \left\lfloor \frac{(p^{r-1} - 1)d}{p^r - 1} \right\rfloor. \tag{7}$$

However, for $i \notin \bigcup_{\mathbf{v}\in\mathsf{F}_q^r\setminus\{\mathbf{0}\}, \mathbf{v}\overline{\mathbf{x}}^0=0} N_{\mathbf{v}}$ we have $L_i(\mathbf{x}^0) \not\equiv 0 \bmod \mathfrak{p}$, hence

$$\operatorname{ord}_{\mathfrak{p}} D(F(p\mathbf{x} + \mathbf{x}^0)) = \operatorname{ord}_{\mathfrak{p}} D\left( \prod_{\substack{\mathbf{v}\in\mathsf{F}_q^r\setminus\{\mathbf{0}\}\\ \mathbf{v}\overline{\mathbf{x}}^0=0}} \prod_{i\in N_{\mathbf{v}}} L_i(p\mathbf{x} + \mathbf{x}^0) \right).$$

Now for $i$ in question, by (6), $\operatorname{ord}_{\mathfrak{p}} C(L_i(p\mathbf{x} + \mathbf{x}^0)) \le \operatorname{ord}_{\mathfrak{p}} p$. Hence by Theorem 1

$$\operatorname{ord}_{\mathfrak{p}} D(F) \le \operatorname{ord}_{\mathfrak{p}} D(F(p\mathbf{x} + \mathbf{x}^0)) \le s(\mathbf{x}^0) \operatorname{ord}_{\mathfrak{p}} p + \operatorname{ord}_{\mathfrak{p}}((s(\mathbf{x}^0))!)$$
$$= \operatorname{ord}_{\mathfrak{p}}((ps(\mathbf{x}^0))!)$$

and the inequality

$$\operatorname{ord}_p\left(\left(p\left\lfloor\frac{(p^{r-1}-1)d}{p^r-1}\right\rfloor\right)!\right) \geq \operatorname{ord}_p D(F)$$

follows from (7).

For the proof of Theorem 3 we need again two lemmas

LEMMA 3. *For all $d$ and $r$ and all primitive forms $F \in \mathsf{Z}[x_1, \dots, x_r]$ of degree $d$*

$$D(F) \mid D_{d,r}.$$

*If, moreover, $F$ splits over $\mathsf{Z}$, then*

$$D(F) \mid D^1_{d,r}.$$

PROOF. We shall prove the first part of the lemma; the proof of the second part is analogous. Assuming the contrary we infer the existence of a prime $p$ such that

$$\operatorname{ord}_p D(F) > \operatorname{ord}_p D_{d,r}.$$

Let $D_{d,r} = D(F_0)$, where $F_0 \in \mathsf{Z}[x_1, \dots, x_r]$ is a primitive form of degree $d$. By the Chinese remainder theorem there exists a form $F_1 \in \mathsf{Z}[x_1, \dots, x_r]$ of degree $d$ satisfying the congruences

$$F_1 \equiv F \bmod p^{\operatorname{ord}_p D(F)},$$
$$F_1 \equiv F_0 \bmod D_{d,r}/p^{\operatorname{ord}_p D_{d,r}}.$$

We have $F_1 = cF_2$, where $F_2$ is primitive and $(c, pD_{d,r}) = 1$. Now, by the congruences above

$$D_{d,r}\, p^{\operatorname{ord}_p D(F) - \operatorname{ord}_p D_{d,r}} \mid D(F_2),$$

hence $D(F_2) > D_{d,r}$, contrary to the definition of $D_{d,r}$.

LEMMA 4. *For all primes $p$ and positive integers $d$ the form of degree $d$*

$$F_{pd}(x, y) = \prod_{i=0}^{d-\left\lfloor\frac{d}{p+1}\right\rfloor-1} (x - iy) \prod_{j=0}^{\left\lfloor\frac{d}{p+1}\right\rfloor-1} (y - jpx)$$

*is primitive and satisfies*

$$\operatorname{ord}_p D(F_{pd}) \geq e_p = \operatorname{ord}_p\left(\left(p\left\lfloor\frac{d}{p+1}\right\rfloor\right)!\right). \tag{8}$$

PROOF. The form $F_{pd}$ is primitive, since each factor is primitive. We consider three cases

$$y \not\equiv 0 \bmod p, \tag{9}$$

$$y \equiv 0 \not\equiv x, \tag{10}$$

$$y \equiv 0 \equiv x \bmod p. \tag{11}$$

In the case (9) there exists an integer $z$ such that

$$x \equiv zy \bmod p^{e_p}.$$

Hence

$$\begin{aligned}\prod_{i=0}^{d-\left\lfloor \frac{d}{p+1}\right\rfloor -1}(x-iy) &\equiv y^{d-\left\lfloor \frac{d}{p+1}\right\rfloor}\prod_{i=0}^{d-\left\lfloor \frac{d}{p+1}\right\rfloor -1}(z-i)\\ &\equiv y^{d-\left\lfloor \frac{d}{p+1}\right\rfloor}\left(d-\left\lfloor\frac{d}{p+1}\right\rfloor\right)!\binom{z}{d-\left\lfloor \frac{d}{p+1}\right\rfloor} \bmod p^{e_p}.\end{aligned}$$

Now,

$$d-\left\lfloor\frac{d}{p+1}\right\rfloor \geq p\left\lfloor\frac{d}{p+1}\right\rfloor,$$

hence

$$\operatorname{ord}_p F_{pd}(x,y) \geq \min\left(\operatorname{ord}_p\left(\left(d-\left\lfloor\frac{d}{p+1}\right\rfloor\right)!\right), e_p\right) \geq e_p.$$

In the case (10) we have $y = pt$, $t \in \mathbf{Z}$ and there exists an integer $u$ such that

$$t \equiv ux \bmod p^{e_p-\left\lfloor \frac{d}{p+1}\right\rfloor}.$$

Hence

$$\begin{aligned}\prod_{j=0}^{\left\lfloor \frac{d}{p+1}\right\rfloor -1}(y-jpx) &= p^{\left\lfloor \frac{d}{p+1}\right\rfloor}\prod_{j=0}^{\left\lfloor \frac{d}{p+1}\right\rfloor -1}(t-jx)\\ &\equiv p^{\left\lfloor \frac{d}{p+1}\right\rfloor}\left\lfloor\frac{d}{p+1}\right\rfloor!\binom{u}{\left\lfloor \frac{d}{p+1}\right\rfloor} \bmod p^{e_p}\end{aligned}$$

and

$$\operatorname{ord}_p F_{pd}(x,y) \geq \left\lfloor\frac{d}{p+1}\right\rfloor + \min\left(\operatorname{ord}_p\left(\left\lfloor\frac{d}{p+1}\right\rfloor!\right), e_p - \left\lfloor\frac{d}{p+1}\right\rfloor\right).$$

Since $p\lfloor \frac{d}{p+1} \rfloor$ and $\lfloor \frac{d}{p+1} \rfloor$ have the same sum of digits in the base $p$, by Lemma 1 the right-hand side equals $e_p$.

In the case (11) we have

$$\operatorname{ord}_p F_{pd}(x, y) \geq d > \frac{d-1}{p-1} \geq \operatorname{ord}_p(d!) \geq \operatorname{ord}_p \left( \left( p \left\lfloor \frac{d}{p+1} \right\rfloor \right)! \right) = e_p.$$

Thus in each case (8) holds.

PROOF OF THEOREM 3. For $r = 2$ the theorem is contained in Lemma 4. For $r \geq 2$ consider the form splitting over $\mathsf{Z}$

$$F_0 = \prod_{\substack{a_1=0 \\ p \nmid (a_1, \ldots, a_r)}}^{pq-1} \ldots \prod_{a_r=0}^{pq-1} (a_1 x_1 + \cdots + a_r x_r).$$

The number of factors in the product is $(p^r - 1)q^r$, hence $\deg F_0 F_{p,d-(p^r-1)q^r} = d$. We have $F_0 F_{p,d-(p^r-1)q^r} = cF_1$, where $c \not\equiv 0 \bmod p$ and $F_1$ is primitive, thus $F_1 \in S^1_{d,r}$ and by Lemma 4

$$\operatorname{ord}_p D^1_{d,r} \geq \operatorname{ord}_p D(F_0) + \operatorname{ord}_p \left( \left( p \left\lfloor \frac{d - (p^r - 1)q^r}{p+1} \right\rfloor \right)! \right).$$

In order to prove that

$$\operatorname{ord}_p D(F_0) \geq (p^{r-1} - 1)q^{r-1} \operatorname{ord}_p((pq)!) \tag{12}$$

we distinguish two cases:

$$x_j \not\equiv 0 \bmod p \qquad \text{for at least one } j \leq r \tag{13}$$

and

$$x_1 \equiv \cdots \equiv x_r \equiv 0 \bmod p. \tag{14}$$

In the case (13) we may assume in view of symmetry between $x_j$ that $x_r \not\equiv 0 \bmod p$. Then there exist integers $y_j$ such that $x_j \equiv y_j x_r \bmod p^d$ $(j < r)$ and

we obtain

$$
\begin{aligned}
&F_0(x_1, \dots, x_r) \\
&\quad \equiv x_r^{(p^r-1)q^r} \prod_{\substack{a_1=0 \\ p\nmid(a_1,\dots,a_r)}}^{pq-1} \cdots \prod_{a_r=0}^{pq-1} (a_1 y_1 + \cdots + a_{r-1} y_{r-1} + a_r) \\
&\quad = x_r^{(p^r-1)q^r} \prod_{\substack{a_1=0 \\ p\nmid(a_1,\dots,a_{r-1})}}^{pq-1} \cdots \prod_{a_{r-1}=0}^{pq-1} (pq)! \binom{a_1 y_1 + \cdots + a_{r-1} y_{r-1} + pq - 1}{pq} \\
&\qquad \cdot \prod_{\substack{a_1=0 \\ p\mid(a_1,\dots,a_{r-1})}}^{pq-1} \cdots \prod_{\substack{a_{r-1}=0 \\ p\mid a_{r-1}}}^{pq-1} \prod_{\substack{a_r=0 \\ p\nmid a_r}}^{pq-1} (a_1 y_1 + \cdots + a_{r-1} y_{r-1} + a_r) \bmod p^d.
\end{aligned}
$$

Since there are $(p^{r-1}-1)q^{r-1}$ vectors $[a_1, \dots, a_{r-1}] \in \{0, \dots, pq-1\}^r$ such that $p \nmid (a_1, \dots, a_{r-1})$ we obtain

$$
\begin{aligned}
\operatorname{ord}_p F_0(x_1, \dots, x_r) &\geq \min\{d, (p^{r-1}-1)q^{r-1} \operatorname{ord}_p((pq)!)\} \\
&= (p^{r-1}-1)q^{r-1} \operatorname{ord}_p((pq)!),
\end{aligned}
$$

hence (12) follows.

In the case (14) the same inequality is obvious.

PROOF OF COROLLARY 1. For $r = 2$ we have $S_{d,r} = S^0_{d,r}$. The upper estimate for $\operatorname{ord}_p D(F)$ given in Theorem 2 and the lower estimate for $\operatorname{ord}_p D^1_{d,2}$ given in Theorem 3 coincide.

REMARK. There exists a more direct proof of Corollary 1 using a factorization of $F$ over the $p$-adic field instead of a factorization over $\mathsf{C}$.

PROOF OF COROLLARY 2. $d_2(n)$ is the least non-negative integer such that $n! \mid D_{d,2}$. By Corollary 1 this divisibility is equivalent to

$$
\operatorname{ord}_p(n!) \leq \operatorname{ord}_p\left(\left(p\left\lfloor \frac{d}{p+1} \right\rfloor\right)!\right) \qquad \text{for all primes } p < d,
$$

or to

$$
\left\lfloor \frac{n}{p} \right\rfloor \leq \left\lfloor \frac{d}{p+1} \right\rfloor.
$$

The least $d$ satisfying this inequality for all primes $p < d$ is

$$
\max_p \left((p+1)\left\lfloor \frac{n}{p} \right\rfloor\right) \geq 3\left\lfloor \frac{n}{2} \right\rfloor
$$

Except for $n = 3$ we have the equality.

PROOF OF COROLLARY 3. We have by Lemma 1

$$\operatorname{ord}_p\left(\left(p\left\lfloor\frac{(p^{r-1}-1)d}{p^r-1}\right\rfloor\right)!\right) < \frac{p(p^{r-1}-1)d}{(p^r-1)(p-1)} = \left(\frac{1}{p-1}-\frac{1}{p^r-1}\right)d.$$

On the other hand, for $d \geq p^r - 1$

$$q^r > \left(\sqrt[r]{\frac{d}{p^r-1}}-1\right)^r > \frac{d}{p^r-1} - r\left(\frac{d}{p^r-1}\right)^{\frac{r-1}{r}}$$

and for $d < p^r - 1$

$$0 > \frac{d}{p^r-1} - r\left(\frac{d}{p^r-1}\right)^{\frac{r-1}{r}},$$

thus by Lemma 1

$$\begin{aligned}
&(p^{r-1}-1)q^{r-1}\operatorname{ord}_p((pq)!) + \operatorname{ord}_p\left(\left(p\left\lfloor\frac{d-(p^r-1)q^r}{p+1}\right\rfloor\right)!\right)\\
&\geq (p^{r-1}-1)\frac{pq^r}{p-1} - (p^{r-1}-1)q^{r-1}\left(\frac{\log d}{\log p}+1\right)\\
&\qquad + \frac{p}{p-1}\cdot\frac{d-(p^r-1)q^r}{p+1} - \frac{\log d}{\log p}\\
&\geq \frac{pd}{p^2-1} + \frac{(p^r-p^2)q^r}{p^2-1} + d^{\frac{r-1}{r}}O\left(\frac{\log d}{r\log p}+1\right)\\
&> d\left(\frac{1}{p-1}-\frac{1}{p^r-1}\right) + d^{\frac{r-1}{r}}O\left(\frac{r}{p}+\frac{\log d}{r\log p}+1\right).
\end{aligned}$$

It is easy to see that for $r = 2$ the factor $d^{\frac{r-1}{r}}$ can be omitted.

PROOF OF COROLLARY 4. By (1) we have

$$\log D_{d,r} \leq \log d! = d\log d + O(d),$$

on the other hand, by Corollary 1,

$$\log D_{d,r} \geq \log D_{d,2} \geq \sum_{\substack{p<d \\ p \text{ prime}}} \left\lfloor \frac{d}{p+1} \right\rfloor \log p$$

$$\geq d \sum_{\substack{p<d \\ p \text{ prime}}} \frac{\log p}{p+1} - \sum_{\substack{p<d \\ p \text{ prime}}} \log p = d \log d + O(d).$$

For the proof of Theorem 4 we need three lemmas.

LEMMA 5. *If, for a prime* $p$,

$$\operatorname{ord}_p D_{d,r+1} > \operatorname{ord}_p D_{d,r}, \tag{15}$$

*then there exists a form* $F \in S_{d,r+1}$ *such that*

$$\operatorname{ord}_p D(F) = \operatorname{ord}_p D_{d,r+1} \tag{16}$$

*and*

$$x_1 x_2 \ldots x_{r+1} \mid F.$$

PROOF. Let

$$D_{d,r+1} = D(F_0), \qquad \text{when} \quad F_0 \in S_{d,r+1}. \tag{17}$$

We have

$$F_0 = \sum_{S \subset \{1,\ldots,r+1\}} F_S,$$

where $F_S$ consists of those monomials of $F$ in which occur just the variables with indices belonging to $S$, $F_\emptyset = 0$. It follows by induction on $s \leq r+1$ that

$$p^{\operatorname{ord}_p D_{d,r+1}} \mid D(F_s) \tag{18}$$

and

$$p \nmid C(F_s), \tag{19}$$

where $F_s = \sum_{\{1,\ldots,s\} \subset S \subset \{1,\ldots,r+1\}} F_S$.

Indeed, for $s = 0$, (18) and (19) follow from (17). Assuming that (18) holds for an $s \leq r$ and putting $x_{s+1} = 0$ we find that

$$p^{\operatorname{ord}_p D_{d,r+1}} \mid D(F_s - F_{s+1}), \tag{20}$$

hence by (18)

$$p^{\operatorname{ord}_p D_{d,r+1}} \mid D(F_{s+1}).$$

Since the form $F_s - F_{s+1}$ depends only on the variables $x_1, \dots, x_s, x_{s+2}, \dots, x_{r+1}$ it follows from (15) and (20) that

$$p \mid C(F_s - F_{s+1}),$$

hence by (19)

$$p \nmid C(F_{s+1}),$$

which completes the inductive proof of (18) and (19). Applying these formulae for $s = r + 1$ we infer that

$$p^{\operatorname{ord}_p D_{d,r+1}} \mid D(F_{r+1}), \qquad p \nmid C(F_{r+1}).$$

The form $F = F_{r+1}C(F_{r+1})^{-1}$ satisfies the conditions of the lemma.

LEMMA 6. *For all positive integers $d$ and $r$ and for all primes $p$*

$$\operatorname{ord}_p D_{d,r+1} \le \max\left\{\operatorname{ord}_p D_{d,r}, \left\lfloor \frac{d-r-1}{p-1} \right\rfloor\right\}.$$

PROOF. If $\operatorname{ord}_p D_{d,r+1} > \operatorname{ord}_p D_{d,r}$ let $F$ be a form of Lemma 5. We have

$$F = \sum_{\mathbf{i}\in\mathbf{I}} a_{\mathbf{i}} \cdot x_1^{i_1} x_2^{i_2} \dots x_{r+1}^{i_{r+1}},$$

where $\mathbf{i} = [i_1, \dots, i_{r+1}]$, $i_s$ $(1 \le s \le r+1)$ are positive integers, $\mathbf{I}$ is a certain finite set and $i_1 + \dots + i_{r+1} = d$, $a_{\mathbf{i}} \in \mathsf{Z}$ for all $\mathbf{i} \in \mathbf{I}$. We have

$$x^i = i!\binom{x}{i} + f_i(x),$$

where $f_i \in \mathsf{Z}[x]$, $\deg f_i < i$, hence

$$F = \sum_{\mathbf{i}\in\mathbf{I}} a_{\mathbf{i}} \prod_{s=1}^{r+1} i_s! \binom{x_s}{i_s} + f_{\mathbf{i}}(x_1, \dots, x_{r+1})$$

where $f_{\mathbf{i}} \in \mathsf{Z}[x_1, \dots, x_{r+1}]$, $\deg f_{\mathbf{i}} < d$. It follows now from Nagell's theorem [5, p. 15] and (16) that

$$p^{\operatorname{ord}_p D_{d,r+1}} \mid \text{g.c.d.}_{\mathbf{i}\in\mathbf{I}}\left(a_{\mathbf{i}} \prod_{s=1}^{r+1} i_s!\right). \tag{21}$$

However, by Lemma 1,

$$\operatorname{ord}_p \prod_{s=1}^{r+1} i_s! = \sum_{s=1}^{r+1} \operatorname{ord}_p i_s! \le \sum_{s=1}^{r+1} \frac{i_s - 1}{p-1} = \frac{d-r-1}{p-1},$$

and since $F \in S_{d,r+1}$

$$\operatorname{ord}_p \operatorname{g.c.d.}_{\mathbf{i}\in\mathbf{I}} \left( a_{\mathbf{i}} \prod_{s=1}^{r+1} i_s! \right) \le \frac{d-r-1}{p-1},$$

hence we obtain from (21)

$$\operatorname{ord}_p D_{d,r+1} \le \left\lfloor \frac{d-r-1}{p-1} \right\rfloor.$$

LEMMA 7. *For all primes* $p < d$

$$\operatorname{ord}_p \left( \left( p \left\lfloor \frac{d}{p+1} \right\rfloor \right)! \right) \ge \left\lfloor \frac{\operatorname{ord}_2 \left( \left( 2 \left\lfloor \frac{d}{3} \right\rfloor \right)! \right)}{p-1} \right\rfloor. \tag{22}$$

PROOF. In order to diminish the number of parentheses we agree to perform factorial after multiplication. For $p = 2$, (22) becomes equality. For $p = 3$, $d < 12$ we verify (22) directly. For $p = 3$, $d = 12k + r$, $0 \le r < 12$, $k \ge 1$ we have

$$\operatorname{ord}_3 \left( 3 \left\lfloor \frac{d}{4} \right\rfloor ! \right) - \left\lfloor \frac{\operatorname{ord}_2 \left( 2 \left\lfloor \frac{d}{3} \right\rfloor ! \right)}{2} \right\rfloor \ge \frac{k - \operatorname{ord}_2 k! + 2 \left\lfloor \frac{r}{4} \right\rfloor - \operatorname{ord}_2 \left( 2 \left\lfloor \frac{r}{3} \right\rfloor ! \right)}{2}$$

$$\ge \frac{k - \operatorname{ord}_2 k! - 1}{2} \ge 0.$$

For $p = 5$, $d = 6k + r$, $0 \le r < 6$, $k \ge 1$ we have

$$\operatorname{ord}_5 \left( 5 \left\lfloor \frac{d}{6} \right\rfloor ! \right) - \left\lfloor \frac{\operatorname{ord}_2 \left( 2 \left\lfloor \frac{d}{3} \right\rfloor ! \right)}{4} \right\rfloor \ge \frac{k - \operatorname{ord}_2 k! - \operatorname{ord}_2 \left( 2 \left\lfloor \frac{r}{3} \right\rfloor ! \right)}{4}$$

$$\ge \frac{k - \operatorname{ord}_2 k! - 1}{4} \ge 0.$$

For $p = 7$, $d < 24$ we verify (22) directly. For $p = 7$, $d = 24k + r$, $0 \le r < 24$, $k \ge 1$ we have

$$\operatorname{ord}_7\left(7\left\lfloor \frac{d}{8}\right\rfloor !\right) - \left\lfloor \frac{\operatorname{ord}_2\left(2\left\lfloor \frac{d}{3}\right\rfloor !\right)}{6}\right\rfloor \ge \frac{3k + 6\left\lfloor \frac{r}{8}\right\rfloor - \operatorname{ord}_2 k! - \operatorname{ord}_2\left(2\left\lfloor \frac{r}{3}\right\rfloor !\right)}{6}$$
$$\ge \frac{3k - \operatorname{ord}_2 k! - 3}{6} \ge 0.$$

For $p < d < 3p$ we have

$$\operatorname{ord}_p\left(p\left\lfloor \frac{d}{p+1}\right\rfloor !\right) \ge \left\lfloor \frac{d}{p+1}\right\rfloor \ge 1,$$
$$\operatorname{ord}_2\left(2\left\lfloor \frac{d}{3}\right\rfloor !\right) \le \operatorname{ord}_2((2p-2)!) \le 2p-3,$$
$$\left\lfloor \frac{\operatorname{ord}_2\left(2\left\lfloor \frac{d}{3}\right\rfloor !\right)}{p-1}\right\rfloor \le 1.$$

For $3p \le d < \frac{9p-3}{2}$ we have

$$\operatorname{ord}_p\left(p\left\lfloor \frac{d}{p+1}\right\rfloor !\right) \ge \left\lfloor \frac{d}{p+1}\right\rfloor \ge 2,$$
$$\operatorname{ord}_2\left(2\left\lfloor \frac{d}{3}\right\rfloor !\right) \le \operatorname{ord}_2((3p-3)!) \le 3p-4,$$
$$\left\lfloor \frac{\operatorname{ord}_2\left(2\left\lfloor \frac{d}{3}\right\rfloor !\right)}{p-1}\right\rfloor \le 2.$$

For $\frac{9p-3}{2} \le d < 6p - 3$ we have

$$\operatorname{ord}_p\left(p\left\lfloor \frac{d}{p+1}\right\rfloor !\right) \ge \left\lfloor \frac{d}{p+1}\right\rfloor \ge 3,$$
$$\operatorname{ord}_2\left(2\left\lfloor \frac{d}{3}\right\rfloor !\right) \le \operatorname{ord}_2((4p-4)!) \le 4p-5,$$
$$\left\lfloor \frac{\operatorname{ord}_2\left(2\left\lfloor \frac{d}{3}\right\rfloor !\right)}{p-1}\right\rfloor \le 3.$$

For $p \geq 11$, $d \geq 6p-3$ we have

$$\operatorname{ord}_p\left(p\left\lfloor\frac{d}{p+1}\right\rfloor!\right) \geq \left\lfloor\frac{d}{p+1}\right\rfloor \geq \frac{d-p}{p+1},$$

$$\operatorname{ord}_2\left(2\left\lfloor\frac{d}{3}\right\rfloor!\right) \leq 2\left\lfloor\frac{d}{3}\right\rfloor - 1 \leq \frac{2}{3}d - 1,$$

hence

$$\begin{aligned}\operatorname{ord}_p\left(p\left\lfloor\frac{d}{p+1}\right\rfloor!\right) - \left\lfloor\frac{\operatorname{ord}_2\left(2\left\lfloor\frac{d}{3}\right\rfloor!\right)}{p-1}\right\rfloor &\geq \frac{d-p}{p+1} - \frac{\frac{2}{3}d-1}{p-1} \\ &= \frac{d(p-5)-3(p^2-2p-1)}{3(p^2-1)} \\ &\geq \frac{(2p-1)(p-5)-p^2+2p+1}{p^2-1} \\ &= \frac{p^2-9p+6}{p^2-1} \geq \frac{7}{30}.\end{aligned}$$

PROOF OF THEOREM 4. (i) We proceed by induction on $r$. Since $D_{d,1} = 1$, for $r = 1$ the assertion holds. Assume that $D_{d,r} \mid (d-1)!$. It for all primes $p : \operatorname{ord}_p D_{d,r+1} \leq \max\{\operatorname{ord}_p D_{d,r}, \operatorname{ord}_p((d-1)!)\}$, we have $D_{d,r+1} \mid (d-1)!$. Otherwise, by Lemma 5, there exists a prime $p$ and a form $F \in S_{d,r+1}$ such that

$$\operatorname{ord}_p D(F) = \operatorname{ord}_p D_{d,r+1} > \operatorname{ord}_p((d-1)!) \tag{23}$$

and

$$x_1 x_2 \ldots x_{r+1} \mid F. \tag{24}$$

Since $F \in S_{d,r+1}$, $F(x_1 \ldots x_r, 1)$ is primitive and by (24) of degree at most $d-1$. Hence by (1)

$$D(F(x_1 \ldots x_{r-1}, 1) \mid (d-1)!.$$

contrary to (23).

(ii) We proceed by induction on $r \geq r_d$. For $r = r_d$ the assertion is obvious. Assume that it is true for the index $r$. If $D_{d,r+1} > D_{d,r}$, then there exists a prime $p < d$ such that

$$\operatorname{ord}_p D_{d,r+1} > \operatorname{ord}_p D_{d,r}$$

and since for $d \geq 4$, $r_d \geq 2$, by Lemma 6 and Corollary 1

$$\left\lfloor \frac{d-r-1}{p-1} \right\rfloor > \operatorname{ord}_p D_{d,r} \geq \operatorname{ord}_p D_{d,r_d}$$
$$\geq \operatorname{ord}_p D_{d,2} = \operatorname{ord}_p \left( \left( p \left\lfloor \frac{d}{p+1} \right\rfloor \right)! \right).$$

It follows that

$$\left\lfloor \frac{\operatorname{ord}_2 \left( \left( 2 \left\lfloor \frac{d}{3} \right\rfloor \right)! \right)}{p-1} \right\rfloor > \operatorname{ord}_p \left( \left( p \left\lfloor \frac{d}{p+1} \right\rfloor \right)! \right),$$

contrary to Lemma 7. Thus $D_{d,r+1} = D_{d,r}$ and, by the inductive assumption, $D_{d,r+1} = D_{d,r_d}$.

PROOF OF COROLLARY 5. Since $D_{d,2} \leq D_{d,r} \leq (d-1)!$ and for $d \leq 6$, $d \neq 5$, $D_{d,2} = (d-1)!$ we infer that $D_{d,r} = D_{d,2}$. It remains to consider $d = 5$ and by (ii) $r = 3$. Since $D_{5,2} = 6$, $(5-1)! = 24$ it suffices to prove that $D_{5,3} \not\equiv 0 \bmod 4$. Assuming the contrary, by Lemma 5, there exists a form $F_0 \in \mathsf{Z}[x, y, z]$ such that $xyz \mid F_0$

$$4 \mid D(F_0), \qquad 2 \nmid C(F_0). \tag{25}$$

We have for some integers $a, b, c, d, e, f$

$$F_0 = xyz(ax^2 + bxy + cy^2 + dxz + eyz + fz^2) \tag{26}$$

and for $x, y, z$ odd

$$4 \mid ax^2 + bxy + cy^2 + dxz + eyz + fz^2.$$

However for $x, y$ odd

$$x^2 \equiv y^2 \equiv 1, \qquad xy \equiv x + y - 1 \bmod 4,$$

thus

$$4 \mid a - b + c - d - e + f + (b+d)x + (b+e)y + (d+e)z$$

and, since this holds for all $x, y, z$ odd we have

$$b \equiv d \equiv e \bmod 2 \tag{27}$$

and

$$a + b + c + d + e + f \equiv 0 \bmod 4. \tag{28}$$

On the other hand, from (25) and (26) for $\langle x, y, z\rangle = \langle 2,1,1\rangle, \langle 1,2,1\rangle, \langle 1,1,2\rangle$

$$c+e+f \equiv 0, \qquad a+d+f \equiv 0, \qquad a+b+c \equiv 0 \bmod 2.$$

It follows from (27) that $a \equiv c \equiv f \bmod 2$, thus $b \equiv d \equiv f \equiv 0 \bmod 2$ and, by (28), $3a \equiv 0 \bmod 2$, $a \equiv c \equiv f \equiv 0 \bmod 2$, contrary to (25).

REMARK. We have $(D(xyz(x+y)(x+z)(x+y+z)(y+z)(y-z)) = 48$. Since $D_{8,2} = 2520$ it follows by Lemma 3 and Theorem 4 (i) that $D_{8,r} = 7!$ for all $r \geq 3$. On the other hand, a complicated computation shows that for all $r \geq 2$, $D_{7,r} = 5! = D_{7,2}$.

PROOF OF COROLLARY 6. We have by Theorem 2 and Corollary 1

$$\operatorname{ord}_2 D^1_{9,3} \leq \operatorname{ord}_2 \left(\left(2\left\lfloor \frac{27}{7}\right\rfloor\right)!\right) = \operatorname{ord}_2 6! = 4 = \operatorname{ord}_2 D^1_{9,2},$$

$$\operatorname{ord}_3 D^1_{9,3} \leq \operatorname{ord}_3 \left(\left(3\left\lfloor \frac{72}{26}\right\rfloor\right)!\right) = \operatorname{ord}_3 6! = 2 = \operatorname{ord}_3 D^1_{9,2}.$$

For $p = 5, 7$ we have by Corollary 1

$$\operatorname{ord}_2 D^1_{9,2} = 1 = \operatorname{ord}_p 8!.$$

For the proof of Theorem 5 we need 5 lemmas.

LEMMA 8. *For all primes $p$ and all integers $r > 1$ and $\alpha > 0$ let $d(r, p^\alpha)$ and $d^1(r, p^\alpha)$ be the least $d$ such that $p^\alpha \mid D_{d,r}$ and $p^\alpha \mid D^1_{d,r}$, respectively. We have*

$$d(r, p^\alpha) \leq d^1(r, p^\alpha) \leq \frac{p^2-1}{p}\left(\alpha + 2\frac{\log \alpha p}{\log p} + 1\right) \qquad \text{if} \quad \alpha \geq p,$$

$$d(r, p^\alpha) \leq d^1(r, p) \leq \alpha(p+1) \qquad \text{if} \quad \alpha < p.$$

*Moreover,*

$$d(r, p^\alpha) \geq \alpha(p-1) + 2.$$

PROOF. By Lemma 1

$$\operatorname{ord}_p((pn)!) \geq \frac{pn}{p-1} - \frac{\log pn}{\log p},$$

hence by Corollary 1

$$\operatorname{ord}_p D^1_{d,2} = e_p \geq \frac{p}{p^2-1}d - \frac{\log d}{\log p} - 1$$

and if $\alpha \geq p$,

$$d \geq \frac{p^2-1}{p}\left(\alpha + 2\frac{\log \alpha p}{\log p} + 1\right)$$

we obtain

$$e_p \geq \alpha + 2\frac{\log \alpha p}{\log p} + 1 - \frac{\log \frac{p^2-1}{p}\left(\alpha + 2\frac{\log \alpha p}{\log p}\right)}{\log p} - 1 \geq \alpha.$$

Thus $\operatorname{ord}_p D_{d,2} \geq \alpha$ and *a fortiori*

$$\operatorname{ord}_p D_{d,r} \geq \alpha.$$

The same is true for $\alpha < p$ provided $d \geq (p+1)\alpha$.

On the other hand, if $p^\alpha \mid D_{d,r}$, we have by Theorem 4(i) and by Lemma 1

$$\alpha \leq \operatorname{ord}_p((d-1)!) \leq \frac{d-2}{p-1},$$

hence $d \geq \alpha(p-1)+2$.

LEMMA 9. *If $c > 1$ and $p > 8/(c-1)$, then $p^\alpha \mid n!$ implies*

$$d(r, p^\alpha) \leq d^1(r, p^\alpha) < cn.$$

PROOF. If $\alpha < p$, then $n \geq \alpha p$ and by Lemma 8

$$d(r, p) \leq d^1(r, p) \leq \alpha(p+1) < \alpha\left(1 + \frac{c-1}{8}\right)p < cn.$$

If $\alpha \geq p$, then again by Lemma 8

$$d^1(r, p^\alpha) \leq \frac{p^2-1}{p}\left(\alpha + 2\frac{\log \alpha p}{\log p} + 1\right).$$

On the other hand, by Lemma 1

$$\alpha = \operatorname{ord}_p n! < \frac{n}{p-1},$$

hence

$$d^1(r, p^\alpha) \leq \frac{p^2-1}{p}\left(\frac{n}{p-1} + 2\frac{\log 2n}{\log p} + 1\right)$$

and

$$\frac{d^1(r, p^\alpha)}{n} \leq \frac{p+1}{p} + 2\frac{p^2-1}{p}\,\frac{\log 2n}{n \log p} + \frac{p^2-1}{pn}.$$

The right hand side is a decreasing function of $n$ and since $n \geq p^2$, $\frac{d(r,p^\alpha)}{n} \leq \frac{d^1(r,p^\alpha)}{n} \leq \frac{p+1}{p} + 6\frac{p^2-1}{p^3} + \frac{p^2-1}{p^3} < 1 + \frac{8}{p} < c$.

LEMMA 10. *The limit* $\ell(r, p) = \lim_{\alpha\to\infty} \frac{d(r,p^\alpha)}{\alpha}$ *exists and satisfies* $\ell(r, p) \geq p - 1$.

PROOF. By Lemma 8 we have

$$\frac{p^2-1}{p} \geq l(r, p) = \liminf_{\alpha\to\infty} \frac{d(r, p^\alpha)}{\alpha} \geq p - 1.$$

For every integer $n$ there exists an integer $\beta_n$ such that

$$d(r, p^{\beta_n}) \leq \left(l(r, p) + \frac{1}{n}\right)\beta_n.$$

If $f \in S_{d,r}$ and $p^{\beta_n} \mid D(f)$, then $p^{q\beta_n} \mid D(f^q)$, where $f^q \in S_{qd,r}$. Hence choosing for an arbitrary integer $\alpha > 0$ an integer $q$ such that $(q-1)\beta_n < \alpha \leq q\beta_n$ we infer that

$$d(r, p^\alpha) \leq qd(r, p^{\beta_n}) < \frac{q\alpha}{q-1}\left(l(r, p) + \frac{1}{n}\right)$$

and for $\alpha > n\beta_n$

$$d(r, p^\alpha) \leq \left(1 + \frac{1}{n}\right)\left(l(r, p) + \frac{1}{n}\right)\alpha.$$

Since $n$ is arbitrary, it follows that

$$\lim_{\alpha\to\infty} \frac{d(r, p^\alpha)}{\alpha} = l(r, p).$$

LEMMA 11. *The limit* $l_r = \lim_{n\to\infty} \frac{d_r(n)}{n}$ *exists.*

PROOF. If $\limsup_{n\to\infty} \frac{d_r(n)}{n} = 1$, then since by Theorem 4(i)

$$\liminf_{n\to\infty} \frac{d_r(n)}{n} \geq 1$$

we have $l_r = 1$. Assume that $\limsup_{n\to\infty} \frac{d_r(n)}{n} = c > 1$. Since $d_r(n) \leq d_2(n) \leq \frac{3}{2}n$ we have $c < \infty$. We shall prove that

$$\lim_{n\to\infty} \frac{d_r(n)}{n} = \max_{p<\frac{16}{c-1}} \frac{l(r, p)}{p-1} =: M. \tag{29}$$

In order to prove (29) it suffices to prove that

$$\limsup_{n\to\infty} \frac{d_r(n)}{n} \leq M \tag{30}$$

and

$$\liminf_{n\to\infty} \frac{d_r(n)}{n} \geq M. \tag{31}$$

Clearly,

$$d_r(n) = \max_{p^\alpha \| n} d(r, p^\alpha).$$

For $p > \frac{16}{c-1}$ we have by Lemma 9

$$d(r, p^\alpha) < \frac{c+1}{2} n,$$

and, since $\frac{c+1}{2} < c$,

$$\limsup_{n\to\infty} \frac{d_r(n)}{n} = \limsup_{n\to\infty} \max_{\substack{p^\alpha \| n \\ p < \frac{16}{c-1}}} \frac{d(r, p^\alpha)}{n}.$$

Since for every $p < \frac{16}{c-1}$, $\varepsilon > 0$ and $\alpha > \alpha(\varepsilon)$

$$d(r, p^\alpha) < (l(r, p) + \varepsilon)\alpha$$

while, by Lemma 1

$$\alpha = \frac{n}{p-1} + O(\log n) \tag{32}$$

we obtain for $n > n_0(\varepsilon)$

$$d(r, p^\alpha) < (M + \varepsilon)n,$$

which gives (30).

In order to prove (31) let $M = \frac{l(r,p)}{p-1}$ for a prime $p$. In view of (32) $n! \mid D_{d,r}$ implies for every $\varepsilon > 0$ and $n > n_1(\varepsilon)$

$$d \geq d(r, p^\alpha) \geq (l(r, p) - \varepsilon)\left(\frac{n}{p-1} + O(\log n)\right) \geq (M - \varepsilon)n + O(\log n),$$

which proves (31).

LEMMA 12. *Let $d_r^1(n)$ be the least $d$ such that $n! \mid D_{d,r}^1$. Then*

$$\lim_{n\to\infty} \frac{d_r^1(n)}{n} = \frac{2^r-1}{2^r-2}.$$

PROOF. We shall prove the lemma in two steps

$$\limsup_{n\to\infty} \frac{d_r^1(n)}{n} \le \frac{2^r-1}{2^r-2} \tag{33}$$

and

$$\liminf_{n\to\infty} \frac{d_r^1(n)}{n} \ge \frac{2^r-1}{2^r-2}. \tag{34}$$

We have

$$d_r^1(n) = \max_{p^\alpha \| n!} d^1(r, p^\alpha).$$

By Lemma 9 for $p > 8(2^n-2)$ we have

$$d^1(r, p^\alpha) < \frac{2^r-1}{2^r-2} n.$$

For $p < 8(2^n-2)$, by Corollary 3 for every $\varepsilon > 0$ and $n > n(\varepsilon)$, $d > \left(\frac{2^r-1}{2^r-2} + \varepsilon\right) n$.

$$\begin{aligned}
\operatorname{ord}_p D_{d,r}^1 &= d\left(\frac{1}{p-1} - \frac{1}{p^r-1}\right) + O\left(d^{\frac{r-1}{r}} \log d\right) \\
&> \left(\frac{2^r-1}{2^r-2} + \varepsilon\right)\left(\frac{1}{p-1} - \frac{1}{p^r-1}\right) + O\left(n^{\frac{r-1}{r}} \log n\right) \\
&> \frac{n}{p-1} + O(\log n) = \alpha.
\end{aligned}$$

This shows (33). In order to prove (34) suppose that for $\varepsilon > 0$ and arbitrarily large $n$

$$d < \left(\frac{2^r-1}{2^r-2} - \varepsilon\right) n.$$

Then by Corollary 3

$$\begin{aligned}
\operatorname{ord}_2 D_{d,r}^1 &< \left(\frac{2^r-1}{2^r-2} - \varepsilon\right)\left(1 - \frac{1}{2^r-1}\right) n + O\left(n^{\frac{r-1}{r}} \log n\right) \\
&< n - O(\log n) = \operatorname{ord}_2 n!.
\end{aligned}$$

PROOF OF THEOREM 5. The Theorem follows from Lemmas 10 and 11.

For the proof of Theorem 6 we need

LEMMA 13. *For every positive integer r*

$$D(G_r) = \prod_{i=1}^{r} i!, \qquad \text{where} \quad G_r = \prod_{i=1}^{r} x_i \prod_{1 \le i \le j \le r} (x_j - x_i).$$

PROOF. See [4] or [3, Lemma 4.1]. The lemma itself is due to H. W. Segar (cf. [2], p. 269).

PROOF OF THEOREM 6. We shall show that for all primes $p$

$$\operatorname{ord}_p D_{d,r} \ge \operatorname{ord}_p(\lceil d - 3(2d)^{3/4} \rceil !). \tag{35}$$

We distinguish three cases:

$$p \le r^{1/2}, \tag{36}$$

$$p > r^{1/2}, \qquad p^2 + p \le d, \tag{37}$$

$$p^2 + p > d. \tag{38}$$

In the case (36) we have $\binom{r+1}{2} \le d$, hence $D(G_r) \mid D_{d,r}$ and by Lemma 13

$$\operatorname{ord}_p D_{d,r} \ge \sum_{i=1}^{r} \operatorname{ord}_p i!.$$

Now, by Lemma 1, for $i > 1$

$$\operatorname{ord}_p i! \ge \frac{i}{p-1} - \left\lceil \frac{\log i}{\log p} \right\rceil,$$

hence

$$\begin{aligned} \operatorname{ord}_p D_{d,r} &\ge \frac{\binom{r+1}{2} - 1}{p-1} - r + 1 - \frac{\sum_{i=p+1}^{r} \log i}{\log p} \\ &\ge \frac{\binom{r+1}{2}}{p-1} - (r-1)(1 + \log r/\log p). \end{aligned}$$

However by the choice of $r$

$$\binom{r+1}{2} \ge d - r, \qquad 2 \le r < \sqrt{2d},$$

while by Lemma 1

$$\operatorname{ord}_p(\lceil d - 3(2d)^{3/4}\rceil !) \le \frac{d - \lceil 3(2d)^{3/4}\rceil}{p-1} \tag{39}$$

and the inequality (35) follows from

$$\lceil 3(2d)^{3/4}\rceil - r - (p-1)(r-1)(1 + \log r/\log p) \ge 3(2d)^{3/4} - 3r^{3/2} > 0.$$

In the case (37) we have

$$\operatorname{ord}_p\left(\left\lfloor \frac{d}{p+1}\right\rfloor !\right) \ge 1,$$

hence by Corollary 1

$$\operatorname{ord}_p D_{d,r} \ge \operatorname{ord}_p D_{d,2} \ge \frac{d}{p+1}$$

and (35) follows from (39) and the inequality

$$\begin{aligned}(p+1)\lceil 3(2d)^{3/4}\rceil - 2d &> (r^{1/2}+1)3(2d)^{3/4} - 2d \\ &> (r+1)^{1/2}3(2d)^{3/4} - 2d \\ &> (2d)^{1/4}3(2d)^{3/4} - 2d = 4d > 0.\end{aligned}$$

In the case (38) we have

$$p^2 > d - 3(2d)^{3/4}.$$

Let $d - \lfloor 3(2d)^{3/4}\rfloor = ap + b$, where $a, b \in \mathbb{Z}$; $0 \le b < p$. Clearly $a < \sqrt{d} < \lfloor 3(2d)^{3/4}\rfloor$, thus

$$d = ap + b + \lfloor 3(2d)^{3/4}\rfloor > ap + a$$

and

$$\operatorname{ord}_p D_{d,2} = \left\lfloor \frac{d}{p+1}\right\rfloor \ge a = \operatorname{ord}_p\big(\lceil d - 3(2d)^{3/4}\rceil !\big).$$

Proof of Corollary 7. For $r \ge \left\lfloor \frac{-1+\sqrt{8d+1}}{2}\right\rfloor$ we have by Theorem 6 and the Stirling formula

$$\log D_{d,r} \ge \log\lceil d - 3(2d)^{3/4}\rceil ! = d\log d - d + O(d^{3/4}\log d).$$

On the other hand, by Theorem 4(i)

$$\log D_{d,r} \le \log(d-1)! = d\log d - d + O(\log d),$$

hence the assertion.

## REFERENCES

1. Bachmann, P., *Niedere Zahlentheorie I*, reprint, Chelsea, New York 1968.
2. Dickson, L. E., *History of the theory of numbers 1*, reprint, Chelsea, New York 1952.
3. Elsholtz, C., *Additive decomposability of multiplicatively defined sets*, Functiones Approx. Comment. Math. 35 (2006), 61–77.
4. Hensel, K., *Über den grössten gemeinsamen Theiler aller Zahlen, welche durch eine ganze Function von n Veränderlichen darstellbar sind*, J. Reine Angew. Math. 116 (1896), 350–356.
5. Nagell, T., *Über zahlentheoretische Polynome*, Norsk. Mat. Tidsskr. 1 (1919), 14–23, see also The Collected Papers of Trygve Nagell, vol. 1, 29–40, Kingston 2002.

INSTITUTE OF MATHEMATICS
POLISH ACADEMY OF SCIENCES
ŚNIADECKICH 8
00-956 WARSAW
POLAND
*E-mail:* schinzel@impan.pl