ΚΕΦΑΛΑΙΟ 1

# Η αριθμητική των διωνυμικών συντελεστών*

D. B. Fuchs & M. B. Fuchs

Κάθε μαθητής γνωρίζει τους τύπους

$$(1+x)^2 = 1 + 2x + x^2,$$
$$(1+x)^3 = 1 + 3x + 3x^2 + x^3.$$

Οι αριθμοί $(1, 2, 1)$, $(1, 3, 3, 1)$, καθώς και αυτοί που προκύπτουν με ανάλογο τρόπο αν υψώσουμε το $(1 + x)$ στην τέταρτη δύναμη, στην πέμπτη δύναμη κ.ο.κ., ονομάζονται *διωνυμικοί συντελεστές*. Το άρθρο αυτό πραγματεύεται διάφορες ιδιότητες των διωνυμικών συντελεστών. Στην πρώτη ενότητα αναπτύσσουμε τη «γενική θεωρία»: Τα περισσότερα από τα θεωρήματα που αποδεικνύουμε εδώ περιλαμβάνονταν στο σχολικό πρόγραμμα. Στη δεύτερη ενότητα θα δείξουμε έναν πολύ εύκολο τρόπο για τον υπολογισμό του υπολοίπου της διαίρεσης ενός διωνυμικού συντελεστή με έναν πρώτο αριθμό. Η τρίτη, και τελευταία, ενότητα πραγματεύεται ορισμένες αξιοσημείωτες ιδιότητες των διωνυμικών συντελεστών. Οι βασικές προτάσεις αυτής της ενότητας διατυπώνονται χωρίς απόδειξη. Ίσως οι αναγνώστες του *Kvant* να προσπαθήσουν να τις αποδείξουν.

## 1. Ορισμός και απλούστερες ιδιότητες των διωνυμικών συντελεστών

Αν το πολυώνυμο $1 + x$ υψωθεί σε κάποια δύναμη $n$, όπου $n$ ένας φυσικός αριθμός, το αποτέλεσμα θα είναι προφανώς ένα πολυώνυμο βαθμού $n$ (δηλαδή η μέγιστη δύναμη στην οποία θα εμφανίζεται υψωμένο το $x$ σε αυτό το

*Το ρωσικό πρωτότυπο δημοσιεύτηκε στο *Kvant* 1970, αρ. 6, σσ. 17–25.

πολυώνυμο θα ισούται με $n$). Για παράδειγμα:

$$\begin{aligned}
(1+x)^0 &= 1,\\
(1+x)^1 &= 1+x,\\
(1+x)^2 &= 1+2x+x^2,\\
(1+x)^3 &= 1+3x+3x^2+x^3,\\
(1+x)^4 &= 1+4x+6x^2+4x^3+x^4,\\
(1+x)^5 &= 1+5x+10x^2+10x^3+5x^4+x^5.
\end{aligned}$$

Οι συντελεστές αυτών των πολυωνύμων ονομάζονται διωνυμικοί συντελεστές, και υπάρχει ένας ειδικός συμβολισμός για αυτούς: Ο συντελεστής του $x^m$ στο $(1+x)^n$ συμβολίζεται $\binom{n}{m}$. Για παράδειγμα, $\binom{2}{1}=2$, $\binom{4}{2}=6$, $\binom{5}{3}=10$. Στα παλιά βιβλία της άλγεβρας, ο αριθμός $\binom{n}{m}$ περιγραφόταν ως «το πλήθος των συνδυασμών από $m$ αντικείμενα τα οποία λαμβάνονται από μια συλλογή $n$ αντικειμένων». Αν και υπάρχουν λόγοι για αυτή την ονομασία, δεν θα τους εξετάσουμε εδώ, καθώς δεν είναι σημαντικοί για τους σκοπούς μας. Επομένως,

$$(1+x)^n = \binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n. \qquad (1)$$

Από αυτή τη σχέση, μπορούμε να βρούμε εύκολα ότι ισχύει επίσης η

$$(a+x)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}x + \binom{n}{2}a^{n-2}x^2 + \cdots + \binom{n}{n}x^n$$

(το μόνο που έχουμε να κάνουμε είναι να εφαρμόσουμε τον παραπάνω τύπο (1) στο $(1+\frac{x}{a})^n$ και έπειτα να πολλαπλασιάσουμε και τα δύο μέλη της εξίσωσης που προκύπτει επί $a^n$). Ο τελευταίος αυτός τύπος ονομάζεται *διώνυμο του Νεύτωνα*. Από εκεί προέρχεται ο όρος «διωνυμικός συντελεστής».

Είναι προφανές ότι οι αριθμοί $\binom{n}{m}$ είναι μη αρνητικοί ακέραιοι και ότι $\binom{n}{m}=0$ για $m>n$ (το πολυώνυμο $(1+x)^n$ είναι βαθμού $n$, οπότε δεν εμφανίζεται σε αυτό όρος $x^m$ με $m>n$). Επιπλέον, είναι εύκολο να διαπιστώσουμε ότι $\binom{n}{0}=\binom{n}{n}=1$. Οι άλλοι διωνυμικοί συντελεστές $\binom{n}{m}$, όπου $0<m<n$, μπορούν να βρεθούν αν υψώσουμε το $1+x$ σε διάφορες δυνάμεις. Οι τιμές τους για $n\le 10$ παρουσιάζονται στον Πίνακα 1.

Όπως βλέπουμε, οι διωνυμικοί συντελεστές αυξάνονται μάλλον γρήγορα. Ο παρατηρητικός αναγνώστης θα διακρίνει ορισμένα μοτίβα στη διάταξη αυτών των αριθμών. Κατά κανόνα, αυτού του είδους τα μοτίβα συνάγονται εύκολα από τον ορισμό των διωνυμικών συντελεστών. Εδώ θα αποδείξουμε μόνο τα πιο σημαντικά. Ας ξεκινήσουμε με το σημαντικότερο όλων, την *ταυτότητα του Pascal*.

Πινακας 1. Διωνυμικοί συντελεστές

| $n$ \ $m$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 1 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | 1 | 2 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | 1 | 3 | 3 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 1 | 4 | 6 | 4 | 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 1 | 5 | 10 | 10 | 5 | 1 | 0 | 0 | 0 | 0 | 0 |
| 6 | 1 | 6 | 15 | 20 | 15 | 6 | 1 | 0 | 0 | 0 | 0 |
| 7 | 1 | 7 | 21 | 35 | 35 | 21 | 7 | 1 | 0 | 0 | 0 |
| 8 | 1 | 8 | 28 | 56 | 70 | 56 | 28 | 8 | 1 | 0 | 0 |
| 9 | 1 | 9 | 36 | 84 | 126 | 126 | 84 | 36 | 9 | 1 | 0 |
| 10 | 1 | 10 | 45 | 120 | 210 | 252 | 210 | 120 | 45 | 10 | 1 |

**Θεωρημα 1** (Ταυτότητα του Pascal)

$$\binom{n}{m} = \binom{n-1}{m} + \binom{n-1}{m-1} \tag{2}$$

*για όλους τους θετικούς φυσικούς αριθμούς* $n, m$.

**Αποδειξη** Εξ ορισμού, το $\binom{n}{m}$ είναι ο συντελεστής του $x^m$ στο πολυώνυμο $(1+x)^n$. Για να βρούμε αυτό τον συντελεστή, θα πρέπει, κατ' αρχήν, να πολλαπλασιάσουμε το πολυώνυμο $1+x$ με τον εαυτό του $n$ φορές. Πολλαπλασιάζοντας το $1+x$ με τον εαυτό του $n-1$ φορές, παίρνουμε το πολυώνυμο

$$1 + \binom{n-1}{1}x + \binom{n-1}{2}x^2 + \cdots + x^{n-1}.$$

Εκτελώντας τον τελικό πολλαπλασιασμό, παίρνουμε

$$\begin{aligned}
(1+x)&\left[1 + \binom{n-1}{1}x + \binom{n-1}{2}x^2 + \cdots + x^{n-1}\right] \\
&= \left[1 + \binom{n-1}{1}x + \binom{n-1}{2}x^2 + \cdots + x^{n-1}\right] \\
&\quad + \left[x + \binom{n-1}{1}x^2 + \binom{n-1}{2}x^3 + \cdots + x^n\right] \\
&= 1 + \left[\binom{n-1}{1} + 1\right]x + \left[\binom{n-1}{2} + \binom{n-1}{1}\right]x^2 + \cdots + x^n.
\end{aligned}$$

Στην τελική εξίσωση, ο συντελεστής του $x^m$ ισούται με $\binom{n-1}{m} + \binom{n-1}{m-1}$. Επομένως,

$$\binom{n}{m} = \binom{n-1}{m} + \binom{n-1}{m-1},$$

που είναι αυτό ακριβώς που θέλαμε να αποδείξουμε. □

Η ταυτότητα του Pascal είναι χρήσιμη για τον υπολογισμό των διωνυμικών συντελεστών. Για παράδειγμα, αν θέλουμε να προσθέσουμε μια ακόμα γραμμή στον πίνακά μας (τη δωδέκατη, αν μετρήσουμε και το μηδέν), το μόνο που έχουμε να κάνουμε είναι να προσθέσουμε κατά ζεύγη τους γειτονικούς αριθμούς στην προηγούμενη γραμμή (την ενδέκατη):

$$\begin{aligned}
\binom{11}{0} &= 1, & \binom{11}{6} &= \binom{10}{6} + \binom{10}{5} = 462,\\
\binom{11}{1} &= \binom{10}{1} + \binom{10}{0} = 11, & \binom{11}{7} &= \binom{10}{7} + \binom{10}{6} = 330,\\
\binom{11}{2} &= \binom{10}{2} + \binom{10}{1} = 55, & \binom{11}{8} &= \binom{10}{8} + \binom{10}{7} = 165,\\
\binom{11}{3} &= \binom{10}{3} + \binom{10}{2} = 165, & \binom{11}{9} &= \binom{10}{9} + \binom{10}{8} = 55,\\
\binom{11}{4} &= \binom{10}{4} + \binom{10}{3} = 330, & \binom{11}{10} &= \binom{10}{10} + \binom{10}{9} = 11,\\
\binom{11}{5} &= \binom{10}{5} + \binom{10}{4} = 462, & \binom{11}{11} &= \binom{10}{11} + \binom{10}{10} = 1.
\end{aligned}$$

Από τα παραπάνω, καταλαβαίνουμε ότι είναι βολικό να γράψουμε τους διωνυμικούς συντελεστές με τη μορφή ενός τριγωνικού πίνακα (βλ. Σχήμα 1), που ονομάζεται *τρίγωνο του Pascal*.

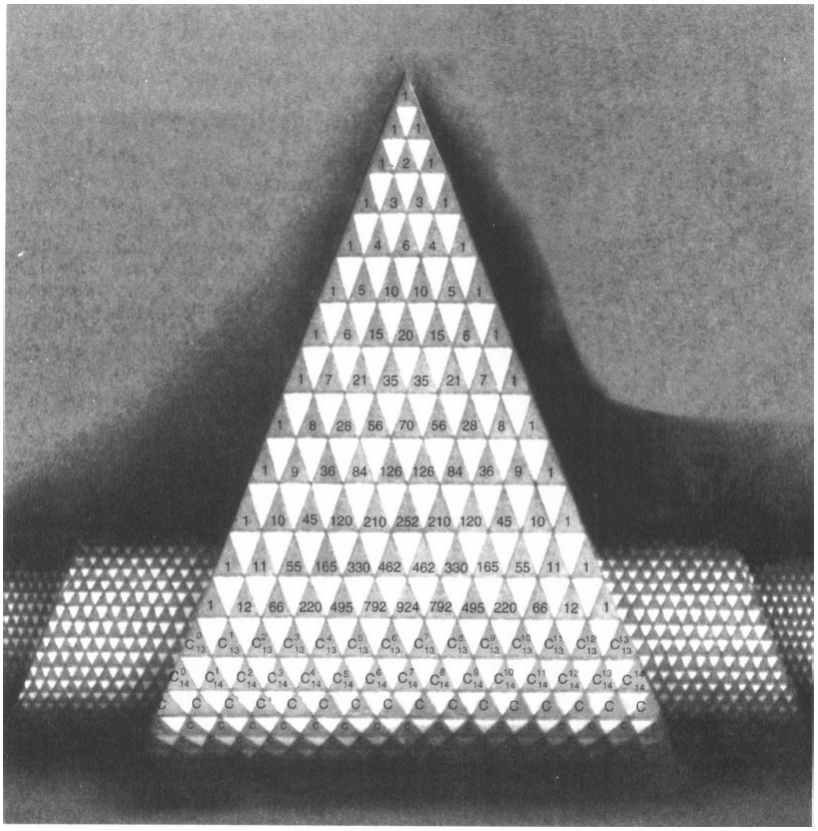
Κάθε αριθμός στο τρίγωνο του Pascal ισούται με το άθροισμα των δύο αριθμών που βρίσκονται από πάνω του (Σ.τ.Ε.:στις άκρες τοποθετείται ο αριθμός 1).

Χρησιμοποιώντας την ταυτότητα του Pascal μπορούμε επίσης να πάρουμε τον γενικό τύπο που εκφράζει το $\binom{n}{m}$ συναρτήσει των $n$ και $m$.

**Θεωρημα 2** (Τύπος για τους διωνυμικούς συντελεστές)*

$$\binom{n}{m} = \frac{n(n-1)\cdots(n-m+1)}{1\cdot 2\cdots m} \tag{3}$$

*Σ.τ.Ε.: Ας παρατηρήσουμε ότι με αυτό τον τύπο μπορούμε να γενικεύσουμε την έννοια του διωνυμικού συντελεστή για οποιοδήποτε $n \in \mathbb{R}^*$.




**Σχήμα 1.** Τρίγωνο του Pascal

*για όλους τους θετικούς φυσικούς αριθμούς $n$ και $m$.*

**Απόδειξη** Θα χρησιμοποιήσουμε τη μέθοδο της μαθηματικής επαγωγής. Αν $n = 1$, τότε ο τύπος (3) ισχύει:

$$\binom{1}{1} = 1 = \frac{1}{1},$$
$$\binom{1}{m} = 0 = \frac{1 \cdot 0 \cdots (1-m+1)}{1 \cdot 2 \cdots m}, \quad m > 1.$$

Ας υποθέσουμε ότι

$$\binom{n-1}{m} = \frac{(n-1)(n-2)\cdots(n-m)}{1 \cdot 2 \cdots m}, \quad m = 1, 2, 3, ...$$

για κάποιο $n$. Τότε, αν $m > 1$,

$$\begin{aligned}\binom{n}{m} &= \binom{n-1}{m} + \binom{n-1}{m-1} \\ &= \frac{(n-1)(n-2)\cdots(n-m+1)(n-m)}{1\cdot 2\cdots(m-1)m} + \frac{(n-1)(n-2)\cdots(n-m+1)}{1\cdot 2\cdots(m-1)} \\ &= \left[\frac{(n-1)(n-2)\cdots(n-m+1)}{1\cdot 2\cdots(m-1)}\right]\cdot\left[\frac{n-m}{m}+1\right] \\ &= \left[\frac{(n-1)(n-2)\cdots(n-m+1)}{1\cdot 2\cdots(m-1)}\right]\cdot\frac{n}{m} \\ &= \frac{n(n-1)(n-2)\cdots(n-m+1)}{1\cdot 2\cdots m}.\end{aligned}$$

Από την άλλη πλευρά, αν $m = 1$, τότε

$$\binom{n}{m} = \binom{n-1}{m} + \binom{n-1}{m-1} = \binom{n-1}{1} + \binom{n-1}{0} = \frac{n-1}{1} + 1 = \frac{n}{1}.$$

Συνεπώς, ο τύπος (3) ισχύει για $n = 1$, και αν ισχύει για $n-1$, ισχύει επίσης για $n$. Αυτό αποδεικνύει τον τύπο (3) για κάθε $n$. □

Συνιστούμε στους αναγνώστες που συναντούν τον τύπο (3) για πρώτη φορά να συναγάγουν από αυτόν τις ισότητες που ήδη γνωρίζουμε: $\binom{n}{0} = \binom{n}{n} = 1$ και $\binom{n}{m} = 0$ για $m > n$.

Ο τύπος (3) παρουσιάζει ήδη ενδιαφέρον λόγω του ότι το κλάσμα που εμφανίζεται στο δεξιό του μέλος ισούται με έναν ακέραιο, δηλαδή όλοι οι αριθμοί στον παρονομαστή απαλείφονται με αριθμούς στον αριθμητή.

Στη συνέχεια παρουσιάζουμε ένα θεώρημα που θα το χρησιμοποιήσουμε παρακάτω.

**Θεωρημα 3** *Αν οι αριθμοί $n$ και $m$ είναι σχετικά πρώτοι, (δηλαδή αν ο μέγιστος κοινός παράγοντας των $n$ και $m$ ισούται με 1), τότε το $\binom{n}{m}$ διαιρείται με το $n$.*

**Αποδειξη**

$$\begin{aligned}\binom{n}{m} &= \frac{n(n-1)(n-2)\cdots(n-m+1)}{1\cdot 2\cdots m} \\ &= \frac{n}{m}\cdot\frac{(n-1)(n-2)\cdots(n-m+1)}{1\cdot 2\cdots(m-1)} \\ &= \frac{n}{m}\cdot\binom{n-1}{m-1}.\end{aligned}$$

Επομένως

$$m\binom{n}{m} = n\binom{n-1}{m-1}.$$

Δηλαδή, ο αριθμός $m\binom{n}{m}$ διαιρείται με το $n$. Αλλά αφού οι $m$ και $n$ είναι σχετικά πρώτοι, δηλαδή ο $m$ δεν διαιρείται με κανένα πρώτο παράγοντα του αριθμού $n$, έπεται ότι το $\binom{n}{m}$ διαιρείται με το $n$. □

Για παράδειγμα, το $\binom{9}{4} = 126$ διαιρείται με το 9, και το $\binom{10}{3} = 120$ διαιρείται με το 10. Ας δούμε μερικές ακόμα ιδιότητες των διωνυμικών συντελεστών:

1. $\binom{n}{m} = \binom{n}{n-m}$.
2. $\binom{m}{m} + \binom{m+1}{m} + \cdots + \binom{m+k}{m} = \binom{m+k+1}{m}$.
3. $\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n$.
4. $\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots = \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \cdots$.

Αφήνουμε τις αποδείξεις αυτών των ιδιοτήτων στον αναγνώστη. (Σ.τ.Ε.: Οι τύποι αυτοί μπορούν να αποδειχθούν και με συνδυαστική).

## 2. Υπόλοιπα στη διαίρεση των διωνυμικών συντελεστών με πρώτους αριθμούς

Σε αυτή την ενότητα (όπως και στην επόμενη) θα χρειαστεί να αναφέρουμε συχνά για δύο αριθμούς ότι «οι ακέραιοι $a$ και $b$ έχουν ίσα υπόλοιπα όταν διαιρούνται με το $p$». Συνήθως, η πρόταση αυτή διατυπώνεται σε συνοπτική μορφή μέσω της έκφρασης $a \equiv b \pmod{p}$. Δηλαδή, ο τύπος $a \equiv b \pmod{p}$ σημαίνει ότι η διαφορά $a-b$ διαιρείται με το $p$. Για παράδειγμα, $4 \equiv 1 \pmod{3}$, και $999999 \equiv 222222 \pmod{7}$. Ο τύπος $a \equiv b \pmod{p}$ μερικές φορές διαβάζεται ως εξής: «Ο αριθμός $a$ είναι ισοϋπόλοιπος με τον $b$, modulo $p$». (Ωστόσο, δεν πρόκειται να χρησιμοποιήσουμε αυτή την έκφραση.)

Δύο προφανείς ιδιότητες του συμβόλου «≡» είναι οι εξής:

1. Αν $a \equiv b \pmod{p}$ και ο $k$ είναι ένας ακέραιος, τότε $ka \equiv kb \pmod{p}$. (Σ.τ.Ε.: Για το αντίστροφο, θα πρέπει οι $k, p$ να είναι σχετικά πρώτοι). Διότι αν το $a-b$ διαιρείται με το $p$, τότε το $ka-kb = k(a-b)$ διαιρείται επίσης με το $p$.

2. Αν $a \equiv b \pmod{p}$ και $b \equiv c \pmod{p}$, τότε $a \equiv c \pmod{p}$. Πράγματι, αν το $a-b$ διαιρείται με το $p$ και το $b-c$ διαιρείται με το $p$, τότε το $a-c = (a-b)+(b-c)$ επίσης διαιρείται με το $p$.

Υπενθυμίζουμε ότι οποιοσδήποτε φυσικός αριθμός $a$ μπορεί να διαιρεθεί με έναν φυσικό αριθμό $p$ «με υπόλοιπο», δηλαδή ο αριθμός $a$ μπορεί να γραφτεί με έναν μοναδικό τρόπο στη μορφή $a = bp + c$, όπου οι $b$ και $c$ είναι ακέραιοι με $0 \leq c < p$.

Ο βασικός σκοπός αυτής της ενότητας είναι να αποδείξουμε την ακόλουθη πρόταση.

**Θεωρημα 4** *Έστω $p$ ένας πρώτος αριθμός, και έστω $m, n$ φυσικοί αριθμοί. Επιπλέον, έστω $k$ και $l$ τα πηλίκα της διαίρεσης των $m$ και $n$, αντίστοιχα, με το $p$, και έστω $s$ και $t$ τα αντίστοιχα υπόλοιπα (δηλαδή, $m = kp+s$ και $n = lp+t$, όπου οι $k, l, s, t$ είναι ακέραιοι και $0 \leq s < p$, $0 \leq t < p$). Τότε*

$$\binom{n}{m} \equiv \binom{l}{k} \cdot \binom{t}{s} \pmod{p}.$$

Όπως θα δούμε παρακάτω, το θεώρημα αυτό μας επιτρέπει να βρούμε υπόλοιπα της διαίρεσης των διωνυμικών συντελεστών με πρώτους αριθμούς σχεδόν χωρίς καθόλου υπολογισμούς.

Πριν από την απόδειξη του Θεωρήματος 4 παραθέτουμε τρία λήμματα.

**Λημμα 1** *Ισχύει η παρακάτω ιδιότητα*:*

$$a^k - b^k = (a-b)(a^{k-1} + a^{k-2}b + \cdots + ab^{k-2} + b^{k-1}).$$

**Αποδειξη** Η απόδειξη είναι προφανής: Εκτελώντας τον πολλαπλασιασμό στο δεξιό μέλος της εξίσωσης και απλοποιώντας ό,τι μπορεί να απλοποιηθεί, παίρνουμε την έκφραση στο αριστερό μέλος. □

**Λημμα 2** *Αν ο $p$ είναι πρώτος αριθμός και $0 < r < p$, τότε το $\binom{p}{r}$ διαιρείται με το $p$ (δηλαδή χωρίς υπόλοιπο).*

**Αποδειξη** Η πρόταση έπεται από το Θεώρημα 3: Αφού ο $p$ είναι πρώτος και $r < p$, οι αριθμοί $r$ και $p$ είναι σχετικά πρώτοι. □

(Να σημειωθεί πως το γεγονός ότι ο αριθμός $p$ είναι πρώτος δεν χρησιμοποιείται πουθενά αλλού στην απόδειξη του Θεωρήματος 4· ωστόσο, για έναν μη πρώτο αριθμό $p$, η πρόταση του θεωρήματος δεν ισχύει.)

**Λημμα 3** *Το πολυώνυμο $(1+x)^p - (1+x^p)$ διαιρείται δια $p$ (με την έννοια ότι κάθε συντελεστής αυτού του πολυωνύμου διαιρείται δια $p$).*

*Η πρόταση αυτή, βέβαια, δεν έχει καμία σχέση με τους διωνυμικούς συντελεστές. Την έχουμε απομονώσει σε ξεχωριστό λήμμα προκειμένου να απλοποιήσουμε την απόδειξη του Θεωρήματος 4.

**Απόδειξη** Πράγματι,

$$\begin{aligned}(1+x)^p-(1+x^p) &= 1+\binom{p}{1}x+\cdots+\binom{p}{p-1}x^{p-1}+x^p-1-x^p\\ &= \binom{p}{1}x+\cdots+\binom{p}{p-1}x^{p-1}.\end{aligned}$$

Η τελευταία έκφραση διαιρείται με το $p$ βάσει του Λήμματος 2. □

Και τώρα προχωράμε στην απόδειξη του Θεωρήματος 4.

**Απόδειξη του Θεωρηματος 4** Έστω το πολυώνυμο

$$P(x)=(1+x)^{lp+t}-(1+x)^t(1+x^p)^l.$$

Το πολυώνυμο αυτό διαιρείται με $p$. Πράγματι, από το Λήμμα 1,

$$\begin{aligned}P(x) &= (1+x)^t\left[(1+x)^{pl}-(1+x^p)^l\right]\\ &= (1+x)^t\left[(1+x)^p-(1+x^p)\right]\left[(1+x)^{p(l-1)}+\cdots+(1+x^p)^{l-1}\right]\end{aligned}$$

Σύμφωνα με το Λήμμα 3, ο δεύτερος παράγοντας διαιρείται με το $p$· επομένως, ολόκληρο το γινόμενο επίσης διαιρείται με το $p$.

Ας προσδιορίσουμε τον συντελεστή του όρου $x^{kp+s}$ στο $P(x)$. Όπως ξέρουμε, το $x^{kp+s}$ εμφανίζεται στο $(1+x)^{lp+t}$ με τον συντελεστή $\binom{lp+t}{kp+s}$. Όσον αφορά το γινόμενο $(1+x)^t(1+x^p)^l$, αυτό είναι ίσο με

$$\begin{aligned}&\left[1+\binom{t}{1}x+\binom{t}{2}x^2+\cdots+x^t\right]\left[1+\binom{l}{1}x^p+\binom{l}{2}x^{2p}+\cdots+x^{lp}\right]\\ &\quad= 1+\binom{t}{1}x+\binom{t}{2}x^2+\cdots+x^t+\binom{l}{1}x^p+\binom{l}{1}\binom{t}{1}x^{p+1}\\ &\qquad+\binom{l}{1}\binom{t}{2}x^{p+2}+\cdots+\binom{l}{1}x^{p+t}+\binom{l}{2}x^{2p}+\binom{l}{2}\binom{t}{1}x^{2p+1}\\ &\qquad+\binom{l}{2}\binom{t}{2}x^{2p+2}+\cdots+\binom{l}{2}x^{2p+t}+\cdots\\ &\qquad+x^{lp}+\binom{t}{1}x^{lp+1}+\binom{t}{2}x^{lp+2}+\cdots+x^{lp+t}.\end{aligned}$$

Δεδομένου ότι $t<p$, έπεται ότι στο τελευταίο άθροισμα καμία δύναμη της μεταβλητής $x$ δεν εμφανίζεται περισσότερες από μία φορές. Συνεπώς, ο συντελεστής του όρου $x^{kp+s}$ ισούται με $\binom{l}{k}\binom{t}{s}$ (ειδικότερα, αν $s>t$, τότε ο συντελεστής αυτός είναι ίσος με μηδέν).

Επομένως, ο συντελεστής του όρου $x^{kp+s}$ στο πολυώνυμο $P(x)$ ισούται με $\binom{lp+t}{kp+s}-\binom{l}{k}\binom{t}{s}$. Δεδομένου ότι το $P(x)$ διαιρείται με το $p$, έπεται ότι ο αριθμός

$\binom{lp+t}{kp+s} - \binom{l}{k}\binom{t}{s}$ επίσης διαιρείται με το $p$, που είναι αυτό ακριβώς που έπρεπε να αποδείξουμε. □

Ας δείξουμε τώρα πώς μπορεί να χρησιμοποιηθεί το θεώρημα που μόλις αποδείξαμε για να βρεθούν τα υπόλοιπα της διαίρεσης των διωνυμικών συντελεστών με πρώτους αριθμούς. Ας υπολογίσουμε, για παράδειγμα, το υπόλοιπο της διαίρεσης του αριθμού $\binom{119}{33}$ με το 5. (Φυσικά, αυτό μπορεί να γίνει επίσης με υπολογισμό του $\binom{119}{33}$ σύμφωνα με τον τύπο (2), αλλά αυτό θα απαιτούσε πολλή δουλειά. Σε τελική ανάλυση, ο $\binom{119}{33}$ είναι ένας 30-ψήφιος αριθμός!)

Διαιρώντας τους αριθμούς 119 και 33 με το 5, παίρνουμε $119 = 23 \cdot 5 + 4$ και $33 = 6 \cdot 5 + 3$. Με βάση το θεώρημα, έχουμε ότι $\binom{119}{33} \equiv \binom{23}{6}\binom{4}{3} \pmod 5$. Με ανάλογο τρόπο μπορούμε να διερευνήσουμε και τον αριθμό $\binom{23}{6}$. Έχουμε $23 = 4 \cdot 5 + 3$, $6 = 1 \cdot 5 + 1$, και συνεπώς $\binom{23}{6} \equiv \binom{4}{1}\binom{3}{1} \pmod 5$. Σύμφωνα με την πρώτη ιδιότητα του συμβόλου $\equiv$ (βλ. την αρχή αυτής της ενότητας), $\binom{23}{6}\binom{4}{3} \equiv \left[\binom{4}{1}\binom{3}{1}\right]\binom{4}{3} \pmod 5$. Σύμφωνα με τη δεύτερη ιδιότητα του συμβόλου $\equiv$, έχουμε ότι $\binom{119}{33} \equiv \binom{4}{1}\binom{3}{1}\binom{4}{3} \pmod 5$. Συνεπώς, ο αριθμός $\binom{119}{33}$ όταν διαιρείται με το 5 έχει το ίδιο υπόλοιπο που έχει και ο $\binom{4}{1}\binom{3}{1}\binom{4}{3} = 4 \cdot 3 \cdot 4 = 48$, δηλαδή τον αριθμό 3.

Με ανάλογο τρόπο μπορούμε να βρούμε τα υπόλοιπα της διαίρεσης του αριθμού $\binom{119}{33}$ με άλλους πρώτους αριθμούς. Για παράδειγμα, όταν $p = 2$:

$$119 = 59 \cdot 2 + 1,\ 33 = 16 \cdot 2 + 1 \Rightarrow \binom{119}{33} \equiv \binom{59}{16}\binom{1}{1} = \binom{59}{16} \pmod 2,$$

$$59 = 29 \cdot 2 + 1,\ 16 = 8 \cdot 2 + 0 \Rightarrow \binom{59}{16} \equiv \binom{29}{8}\binom{1}{0} = \binom{29}{8} \pmod 2,$$

$$29 = 14 \cdot 2 + 1,\ 8 = 4 \cdot 2 + 0 \Rightarrow \binom{29}{8} \equiv \binom{14}{4}\binom{1}{0} = \binom{14}{4} \pmod 2,$$

$$14 = 7 \cdot 2 + 0,\ 4 = 2 \cdot 2 + 0 \Rightarrow \binom{14}{4} \equiv \binom{7}{2}\binom{0}{0} = \binom{7}{2} \pmod 2,$$

$$7 = 3 \cdot 2 + 1,\ 2 = 1 \cdot 2 + 0 \Rightarrow \binom{7}{2} \equiv \binom{3}{1}\binom{1}{0} = \binom{3}{1} = 3 \pmod 2.$$

Επομένως, ο αριθμός $\binom{119}{33}$ όταν διαιρείται με το 2 έχει το ίδιο υπόλοιπο που έχει και ο 3, δηλαδή υπόλοιπο 1· με άλλα λόγια, ο $\binom{119}{33}$ είναι περιττός αριθμός.

Άλλο παράδειγμα ($p = 3$):

$$119 = 39 \cdot 3 + 2,\ 33 = 11 \cdot 3 + 0 \Rightarrow \binom{119}{33} \equiv \binom{39}{11}\binom{2}{0} = \binom{39}{11} \pmod 3,$$

$$39 = 13 \cdot 3 + 0,\ 11 = 3 \cdot 3 + 2 \Rightarrow \binom{39}{11} \equiv \binom{13}{3}\binom{0}{2} = 0 \pmod 3.$$

Εδώ χρησιμοποιήσαμε το γεγονός ότι $\binom{0}{2} = 0$, αφού $2 > 0$. Βλέπουμε λοιπόν ότι $\binom{119}{33} \equiv 0 \pmod 3$, δηλαδή ο $\binom{119}{33}$ διαιρείται με το 3.

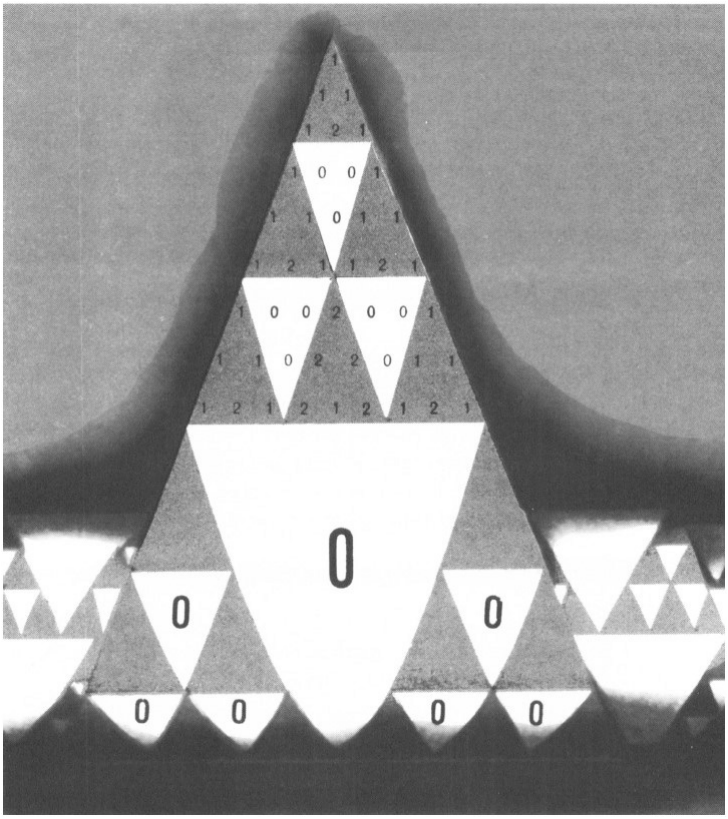
Να σημειωθεί ότι αν εφαρμόσουμε το Θεώρημα 4 στο $\binom{n}{m}$, όπου $n \geq m$, τότε γράφοντας $m = kp + s$, $n = lp + t$, θα πάρουμε φυσικά $l \geq k$· ωστόσο, είναι αδύνατο να προβλέψουμε ποιος από τους αριθμούς $s, t$ θα προκύψει μεγαλύτερος. Αν $s > t$, τότε με βάση το θεώρημά μας $\binom{n}{m} \equiv \binom{l}{k}\binom{t}{s} = 0 \pmod p$. Δηλαδή, το $\binom{n}{m}$ διαιρείται με το $p$. Όπως έχουμε δει, για να προσδιοριστεί το υπόλοιπο της διαίρεσης του αριθμού $\binom{n}{m}$ με το $p$, το Θεώρημα 4 θα πρέπει εν γένει να εφαρμοστεί πολλές φορές. Κάθε φορά μπορεί να προκύψει η κατάσταση που μόλις περιγράψαμε, και, επιπλέον, όποτε κι αν συμβεί αυτό, θα σημαίνει ότι ο *αρχικός* μας αριθμός, $\binom{n}{m}$, διαιρείται με το $p$. Με αυτόν ακριβώς τον τρόπο προσδιορίσαμε ότι το $\binom{119}{33}$ διαιρείται με το 3.

Όπως καταλαβαίνουμε, όσο μεγαλύτερο είναι το $n$, τόσο πιο πιθανό είναι ο αριθμός $\binom{n}{m}$ να διαιρείται με $p$. Μπορούμε να αποδείξουμε εύκολα την παρακάτω, ακριβέστερη πρόταση: Συνολικά, υπάρχουν $\frac{p^r(p^r+1)}{2}$ αριθμοί $\binom{n}{m}$, με $0 \leq n \leq p^r,\ 0 \leq m \leq n$, από τους οποίους ακριβώς $\frac{p^r(p+1)^r}{2^r}$ δεν διαιρούνται με το $p$ (εδώ το $p$ είναι πρώτος και ο $r$ είναι φυσικός αριθμός· η απόδειξη –την οποία αφήνουμε για τον αναγνώστη– απαιτεί μόνο τη χρήση του Θεωρήματος 3). Θα πρέπει να τονίσουμε ότι για μεγάλους αριθμούς $r$, ο αριθμός $\frac{p^r(p+1)^r}{2^r}$ είναι πολλές φορές μικρότερος του $\frac{p^r(p^r+1)}{2}$. (Σ.τ.Ε.: Σχηματίζουμε τον λόγο αυτών των αριθμών και παίρνουμε το όριο για $r \to +\infty$). Επομένως, για παράδειγμα, από τους αριθμούς $\binom{n}{m}$ με $0 \leq n \leq 3^5$, $0 \leq m \leq n$, περίπου το $26{,}2\,\%$ δεν διαιρούνται με το 3. Για $0 \leq n \leq 3^{10}$, το ποσοστό είναι κατά προσέγγιση $3{,}6\,\%$, και για $0 \leq n \leq 3^{15}$, είναι κατά προσέγγιση $0{,}45\,\%$.

Ολοκληρώνοντας, ας πούμε κάποια πράγματα και για τη γραφική αναπαράσταση του Θεωρήματος 4 μέσω του «τριγώνου του Pascal modulo $p$». Πρόκειται για τον πίνακα που προκύπτει από το τρίγωνο του Pascal αν αντικαταστήσουμε κάθε αριθμό με το υπόλοιπο της διαίρεσής του με το $p$. Δεν θα αποδείξουμε κανένα θεώρημα σχετικά με αυτό το τρίγωνο, αλλά θα αρκεστούμε να παρουσιάσουμε στον αναγνώστη το Σχήμα 2, το τρίγωνο του Pascal modulo 3. Σκεφτείτε τι μορφή έχουν τα τμήματα αυτών των τριγώνων που δεν εμφανίζονται στο σχήμα. Προσπαθήστε να διατυπώσετε το Θεώρημα 4 με τέτοιο τρόπο ώστε να μετατραπεί σε θεώρημα για το τρίγωνο του Pascal modulo $p$.

## 3. Σύντομη παρέκβαση στα υπόλοιπα των διαιρέσεων των διωνυμικών συντελεστών με δυνάμεις πρώτων αριθμών

Δεν θα ασχοληθούμε σε πολύ γενικό επίπεδο με τις ιδιότητες των υπολοίπων της διαίρεσης των διωνυμικών συντελεστών με σύνθετους αριθμούς. (Εντούτοις, οι αναγνώστες μπορούν να μελετήσουν μόνοι τους το θέμα αυτό. Για πα-



**Σχήμα 2.** Τρίγωνο του Pascal modulo 3.

ράδειγμα, ποιο είναι το υπόλοιπο της διαίρεσης του αριθμού $\binom{119}{33}$ με το 4; Είναι 1 ή 3;) Θα περιοριστούμε να εξετάσουμε ένα αξιοσημείωτο και ακόμη όχι πλήρως κατανοητό φαινόμενο.

Ας ξεκινήσουμε με μερικούς υπολογισμούς. Χρησιμοποιώντας τον τύπο (1) για τους διωνυμικούς συντελεστές, έχουμε ότι

$$\binom{2}{1} = 2, \qquad \binom{4}{2} = 6, \qquad \binom{8}{4} = 70,$$

$$\binom{16}{8} = 12.870, \qquad \binom{32}{16} = 601.080.390.$$

(Ο αναγνώστης θα παρατήρησε, ασφαλώς, ότι οι αριθμοί $1, 2, 4, 8, 16, 32, \ldots$ είναι διαδοχικές δυνάμεις του 2.) Οι ίδιοι οι αριθμοί που προκύπτουν δεν είναι καθόλου αξιοσημείωτοι. Οι διαδοχικές διαφορές τους, όμως, παρουσιάζουν

εκπληκτικές ιδιότητες. Ας δούμε μερικές από αυτές:

$$\begin{aligned} 6-2 &= 4 = 2^2, \\ 70-6 &= 64 = 2^6, \\ 12.870-70 &= 12.800 = 2^9 \cdot 25, \\ 601.080.390-12.870 &= 601.067.520 = 2^{12} \cdot 146.745. \end{aligned}$$

Όπως βλέπουμε, οι διαφορές αυτές διαιρούνται από μεγάλες δυνάμεις του 2, τόσο μεγάλες που είναι απίθανο να πρόκειται για απλή σύμπτωση. Πράγματι, μπορούμε να αποδείξουμε ένα θεώρημα που εξηγεί τουλάχιστον εν μέρει αυτό το φαινόμενο.

**Θεωρημα 5** *Για $n > 1$, ο αριθμός*

$$\alpha_n = \binom{2^{n+1}}{2^n} - \binom{2^n}{2^{n-1}}$$

*διαιρείται δια $2^{2n+2}$.*

**Σχολια**

1. Η υπόθεση ότι $n > 1$ είναι σημαντική, αφού το $\alpha_1$ ισούται με $4$ και δεν διαιρείται με το $2^{2\cdot 1+2} = 2^4 = 16$.

2. Φαίνεται εύλογο ότι για $n > 1$, το $\alpha_n$ διαιρείται ακόμα και με $2^{3n}$: Αυτό ισχύει για $n = 2, 3, 4$, αλλά είναι κάτι που κανείς μας δεν έχει καταφέρει να αποδείξει αν ισχύει στη γενική περίπτωση.

**Αποδειξη του Θεωρηματος 5** Ας ξεκινήσουμε με τη γενική παρατήρηση ότι αν ο αριθμός $r$ είναι περιττός, τότε ο $\binom{2^n}{r}$ διαιρείται με $2^n$. Πράγματι, αφού ο $r$ είναι περιττός και το $2^n$ δεν έχει άλλους πρώτους παράγοντες εκτός από το 2, οι αριθμοί $r$ και $2^n$ είναι σχετικά πρώτοι, και η πρόταση έπεται από το Θεώρημα 3.

Στη συνέχεια, ας ορίσουμε

$$P(x) = (1+x)^{2^{n+1}} - (1-x^2)^{2^n}.$$

Ο όρος $x^{2^n}$ στο πολυώνυμο $P(x)$ έχει συντελεστή $\binom{2^{n+1}}{2^n} - \binom{2^n}{2^{n-1}} = \alpha_n$. (Εδώ χρησιμοποιούμε το γεγονός ότι $n > 1$: Υψώνοντας το $(1-x^2) = 1 + (-x^2)$ στη δύναμη $2^n$, παίρνουμε ως παράγοντα για τον συντελεστή $\binom{2^n}{2^{n-1}}$ όχι το $x^{2^n}$, αλλά το $(-x^2)^{2^{n-1}} = (-1)^{2^{n-1}} x^{2^n}$, και ο αριθμός $(-1)^{2^{n-1}}$ ισούται με $1$ όταν $n > 1$ και με $-1$ όταν $n = 1$.)

Από την άλλη πλευρά,

$$\begin{aligned} P(x) &= (1+x)^{2^{n+1}} - (1+x)^{2^n}(1-x)^{2^n} \\ &= (1+x)^{2^n}\left[(1+x)^{2^n} - (1-x)^{2^n}\right]. \end{aligned}$$

Αλλά:

$$\begin{aligned} (1+x)^{2^n} - (1-x)^{2^n} &= (1+x)^{2^n} - (1+(-x))^{2^n} \\ &= 1 + \binom{2^n}{1}x + \binom{2^n}{2}x^2 + \binom{2^n}{3}x^3 + \cdots + x^{2^n} \\ &\quad - 1 - \binom{2^n}{1}(-x) - \binom{2^n}{2}(-x)^2 \\ &\quad - \binom{2^n}{3}(-x)^3 - \cdots - (-x)^{2^n} \end{aligned}$$

(και αφού το $(-x)^k$ ισούται με $x^k$ όταν το $k$ είναι άρτιο και με $-x^k$ όταν το $k$ είναι περιττό)

$$\begin{aligned} &= 2\left[\binom{2^n}{1}x + \binom{2^n}{3}x^3 + \binom{2^n}{5}x^5 + \cdots \right. \\ &\quad \left. + \binom{2^n}{2^n-1}x^{2^n-1}\right]. \end{aligned}$$

Να σημειωθεί ότι το $x$ εμφανίζεται στο τελικό πολυώνυμο μόνο σε περιττές δυνάμεις.

Θέλουμε να βρούμε τον συντελεστή του $x^{2^n}$ στο $P(x)$, δηλαδή στο γινόμενο

$$\begin{aligned} &(1+x)^{2^n}\left[(1+x)^{2^n} - (1-x)^{2^n}\right] \\ &\quad = 2\left(1 + \binom{2^n}{1}x + \binom{2^n}{2}x^2 + \binom{2^n}{3}x^3 + \cdots + x^{2^n}\right) \\ &\qquad \times \left(\binom{2^n}{1}x + \binom{2^n}{3}x^3 + \binom{2^n}{5}x^5 + \cdots + \binom{2^n}{2^n-1}x^{2^n-1}\right). \end{aligned}$$

Προφανώς, ο όρος $x^{2^n}$ μπορεί να προκύψει με πολλαπλασιασμό του όρου $x^{2^n-1}$ από τον πρώτο παράγοντα επί τον όρο $x$ από τον δεύτερο, με πολλαπλασιασμό του όρου $x^{2^n-3}$ από τον πρώτο παράγοντα επί τον όρο $x^3$ από τον δεύτερο κ.ο.κ. Με αυτό τον τρόπο, ο συντελεστής του $x^{2^n}$ στο $P(x)$, ο οποίος, όπως γνωρίζουμε, ισούται με $\alpha_n$, ισούται επίσης με

$$2\left[\binom{2^n}{1}\binom{2^n}{2^n-1} + \binom{2^n}{3}\binom{2^n}{2^n-3} + \cdots + \binom{2^n}{2^n-1}\binom{2^n}{1}\right].$$

Όπως γνωρίζουμε, καθένας από τους αριθμούς $\binom{2^n}{1}, \binom{2^n}{3}, \dots, \binom{2^n}{2^n-1}$ διαιρείται με το $2^n$. Συνεπώς, καθένας από τους όρους μέσα στις αγκύλες διαιρείται με το $2^n \cdot 2^n = 2^{2n}$. Επιπλέον, μπροστά από την όλη έκφραση έχουμε ένα 2, ενώ επιπλέον ο κάθε όρος μέσα στις αγκύλες εμφανίζεται δύο φορές. Συνεπώς, το $\alpha_n$ διαιρείται με το $2^{2n+2}$, που είναι αυτό που θέλαμε να αποδείξουμε. □

Άρα, το παράξενο φαινόμενο της διαιρετότητας των αριθμών $\alpha_n$ από μεγάλες δυνάμεις του δύο έχει εξηγηθεί σε κάποιο βαθμό. Αλλά κάτι παρόμοιο μπορεί να παρατηρηθεί όταν το 2 αντικατασταθεί από το 3, το 5 ή το 7. Πράγματι,

$$\begin{aligned}
\binom{9}{3} - \binom{3}{1} &= 84 - 3 = 3^4, \\
\binom{27}{9} - \binom{9}{3} &= 4.686.825 - 84 = 4.686.741 = 3^7 \cdot 2.143, \\
\binom{81}{27} - \binom{27}{9} &= 2.306.279.447.501.851.002.720 - 4.686.825 \\
&= 2.306.279.447.501.846.315.895 \\
&= 3^{10} \cdot 39.057.044.954.221.855, \\
\binom{25}{5} - \binom{5}{1} &= 43.130 - 5 = 43.125 = 5^5 \cdot 69, \\
\binom{49}{7} - \binom{7}{1} &= 85.900.584 - 7 = 85.900.577 = 7^5 \cdot 5.111.
\end{aligned}$$

Εν ολίγοις, φαίνεται πως για πρώτους αριθμούς $p$ ο ακέραιος

$$\binom{p^{n+1}}{p^n} - \binom{p^n}{p^{n-1}}$$

διαιρείται με μια μεγάλη δύναμη του αριθμού $p$. Αλλά προς το παρόν κανείς μας δεν έχει σκεφτεί πώς μπορεί να αποδειχθεί αυτό το γεγονός. *

Παρεμπιπτόντως, αν ο $p$ δεν είναι πρώτος, τότε δεν υπάρχει κανένα τέτοιο φαινόμενο. Για παράδειγμα, ο αριθμός

$$\binom{16}{4} - \binom{4}{1} = 1820 - 4 = 1816$$

δεν διαιρείται καν με $4^2$, και ο

$$\binom{36}{6} - \binom{6}{1} = 1.947.792 - 6 = 1.947.786$$

δεν διαιρείται καν με $6^2$.

*Βλ. το άρθρο του Shirshov σε αυτό τον τόμο, σσ. 61-68.

Θεωρούμε σίγουρο πως κάποιος αναγνώστης του *Kvant* θα καταφέρει να διαλευκάνει αυτό το περίπλοκο ερώτημα της αριθμητικής των διωνυμικών συντελεστών.