EEN BEWIJS VOOR DE KLEINE STELLING VAN FERMAT

LEMMA
Als de natuurlijke getallen a en b onderling ondeelbaar zijn, dan laten de b – 1 eerste veelvouden van

$$1a, 2a, 3a, \ldots, ma, \ldots, na, \ldots, (b-1)a \qquad (1)$$

bij deling door b, als resten 1, 2, 3, …, b – 1 over, in een of andere volgorde.

BEWIJS
Die delingen laten b – 1 resten over, alle kleiner dan b.

- Geen enkele van die resten is nul. Immers a en b zijn onderling ondeelbaar en indien b een deler was van een van de termen uit (1), bijvoorbeeld van ma, dan zou b een deler zijn van m. Dit is onmogelijk omdat m kleiner is dan b.
- Alle resten zijn verschillend. Indien immers ma en na dezelfde rest zouden overlaten bij deling door b, dan zou (n – m)a deelbaar zijn door b. Dit is onmogelijk aangezien b onderling ondeelbaar is met a en omdat n – m kleiner is dan b.

KLEINE STELLING VAN FERMAT
Als het priemgetal p het natuurlijk getal a niet deelt, dan is $a^{p-1} - 1$ een p-voud.

BEWIJS
We delen de eerste p – 1 veelvouden van a door p en stellen de resten voor door $r_1, r_2, \ldots, r_{p-1}$. Dan is

$$a = \text{p-voud} + r_1,\ 2a = \text{p-voud} + r_2, \ldots, (p-1)a = \text{p-voud} + r_{p-1}. \qquad (2)$$

Aangezien het priemgetal p het getal a niet deelt, is p onderling ondeelbaar met a, zodat we het lemma kunnen toepassen. De getallen $r_1, r_2, \ldots, r_{p-1}$ zijn dus de getallen 1, 2, …, p in een of andere volgorde.
Door de overeenkomstige leden van de p – 1 gelijkheden (2) lid aan lid met elkaar te vermenigvuldigen, vinden we dat

$$(p-1)!\ a^{p-1} = \text{p-voud} + (p-1)!$$

of

$$(p-1)!\ (a^{p-1} - 1) = \text{p-voud}.$$

Het linkerlid van deze gelijkheid is dus deelbaar door p en bestaat uit de twee factoren (p – 1)! en $a^{p-1} - 1$. Aangezien (p – 1)! = 1.2. 3 … (p – 1) niet deelbaar is door p (omdat geen enkele factor in dat product deelbaar is door p), is $a^{p-1} - 1$ deelbaar door p.

GEVOLG
Is p een priemgetal en a een willekeurig natuurlijk getal, dan is $a^p - a$ een p-voud.
Immers, $a^p - a = a(a^p - 1)$. Ofwel deelt p het getal a en dan deelt p ook $a^p - a$, ofwel deelt p het getal a niet en dan is volgens de bovenstaande stelling p een deler van $a^p - 1$ en dus ook van $a^p - a$.