

Rozważmy sytuację, w której mamy dane dwa rodzaje monet o nominałach całkowitych równych p , q . Zakładamy, że liczby te są względnie pierwsze oraz posiadamy nieskończenie wiele monet każdego rodzaju.

Problem 1. *Czy istnieje taka liczba całkowita, że każda liczba całkowita nie mniejsza od niej jest kwotą, którą możemy zapłacić monetami p i q bez wydawania reszty. Jeśli tak, to ile wynosi najmniejsza spośród nich?*

Ten dość znany problem sprowadza się do wyznaczenia takiej liczby całkowitej, że dla każdej niemniejszej liczby całkowitej n istnieją takie nieujemne liczby całkowite a , b , że $n = ap + bq$. Takie przedstawienie nazwiemy *dobrym*. Przez parę właściwą dla danej liczby n będziemy rozumieć parę liczb, z których jedna pomnożona przez p da n , po dodaniu drugiej pomnożonej przez q . Liczby te będziemy nazywać odpowiednio liczbą a , oraz liczbą b pary właściwej. Parą maksymalną liczby n nazwiemy jedną z par właściwych tej liczby, w której a jest możliwie największe. Będziemy ją oznaczać przez (a_n, b_n) . Powiemy że a jest właściwa dla n gdy a należy do jednej z par właściwych liczby n . Podobnie b jest właściwa dla n gdy należy do pewnej pary właściwej liczby n .

Twierdzenie 1. (Frobeniusa) *Dla dowolnej liczby całkowitej $n \geq (p-1)(q-1)$ istnieje przedstawienie dobre.*

Zanim przejdziemy do dowodu, rozważmy następujący lemat:

Lemat 1. *Dane są liczby względnie pierwsze p , q . Wtedy ciąg reszt z dzielenia $0, p, 2p, \dots, (q-1)p$ przez q , jest permutacją ciągu $0, 1, 2, \dots, q-1$.*

Dowód lematu 1. Załóżmy, że pewne dwie spośród liczb $0, p, 2p, \dots, (q-1)p$ dają tę samą resztę z dzielenia przez q . Niech będą to kp oraz lp . Wówczas różnica $kp - lp$ dzieli się przez q . Jest jednak równa $p(k-l)$ co jest iloczynem liczby względnie pierwszej z q , oraz liczby mieszczącej się w przedziale $< 1-q, q-1 >$ co jest niesprzeczne tylko wtedy, gdy $k-l = 0$, czyli $k = l$. Mamy więc q możliwych liczb w q -elementowym ciągu reszt z dzielenia $0, p, 2p, \dots, (q-1)p$ przez q , w którym wszystkie wyrazy są różne. To już daje tezę.

Dowód twierdzenia 1. Bez straty ogólności można założyć, że $p > q$. Rozważmy ciąg $0, p, 2p, \dots, (q-1)p$. Na mocy lematu 1, pewien jego wyraz daje tę samą resztę z dzielenia przez q co n . Jeśli $n \geq (q-1)p$, to w ciągu $n, n-p, n-2p, \dots, n-(q-1)p$ wystąpi liczba podzielna przez q . Wyrazy tego ciągu są ponadto nieujemne, bo dla dowolnego wyrazu $n - kp \geq (q-1)p - (q-1)p = 0$. Zauważmy teraz, że liczby $pq - p$, $pq - p - q$ dają resztę $-p$ z dzielenia przez q , a żadna liczba pomiędzy nimi nie. Stąd jeśli $(p-1)(q-1) \leq n < (q-1)p$ to w ciągu $n, n-p, n-2p, \dots, n-(q-2)p$ wystąpi liczba podzielna przez q . Wszystkie jego wyrazy są nieujemne, gdyż dla dowolnego wyrazu: $n - kp \geq (p-1)(q-1) - (q-2)p = p - q + 1 > 0$. Dla pewnych nieujemnych a , b zachodzi więc równość $n - ap = bq$, co daje tezę.

Zauważmy też, że liczba $pq - p - q$ nie ma przedstawienia dobrego. Daje ona resztę $-p$ z dzielenia przez q , więc przeprowadzając rozumowanie podobne jak w dowodzie twierdzenia 1, stwierdzilibyśmy, że $a = (q-1)$, oraz $b = (p-1)$. Jednak wtedy $ap + bq = 2pq - p - q$, co jest sprzeczne.

Przyjmijmy od teraz, że liczba n w dowodach to pewna liczba, której pary właściwe będą rozważane, to jest to liczba, która na pewno ma przedstawienie dobre.

Prawdą jest, że dane a jest właściwe dla n wtedy i tylko wtedy, gdy $n - ap$ dzieli się przez q . Korzystając więc z lematu 1 możemy wywnioskować, że wszystkie a , takie że $n - ap$ dzieli się przez q , dają tę samą resztę z dzielenia przez q . Stąd wszystkie takie a różnią się o wielokrotność q . Ciąg wszystkich a właściwych dla n jest więc dany wzorem $a = a_n - kq$, oczywiście dla wszystkich takich k całkowitych, że $a_n - kq \geq 0$. Obliczamy, że wówczas $bq = n - ap = a_n p + b_n q - (a_n - kq)p = (b_n + kp)q$. Wszystkie pary właściwe n są dane wzorem $(a, b) = (a_n - kq, b_n + kp)$. Wartości k są równe kolejnym liczbom naturalnym, gdzie najmniejsza to 0.

Lemat 2. *Dla danej liczby całkowitej $n \geq pq$ istnieje dokładnie m przedstawień dobrych wtedy i tylko wtedy, gdy dla liczby $n - pq$ istnieje dokładnie $m - 1$ przedstawień dobrych.*

Dowód lematu 2. Parą maksymalną dla n jest $(a_{n-pq} + q, b_{n-pq})$, gdyż para ta jest właściwa dla n , a gdyby istniała para w której a jest większe niż $a_{n-pq} + q$ (oczywiście o wielokrotność q), to w tej parze b byłoby mniejsze, równe pewnemu $b_{n-pq} - lp$. W tym wypadku $n - pq - (b_{n-pq} - lp)q = a_{n-pq}p + lpq$. Otrzymalibyśmy większą liczbę właściwą a dla $n - pq$ od tej w parze maksymalnej co jest sprzeczne. Stąd wszystkie pary właściwe dla n są postaci $(a_{n-pq} + q - kq, b_{n-pq} + kp)$. Stąd k może przyjmować o jedną wartość więcej niż w przypadku liczby par właściwych $n - pq$, co pociąga za sobą tezę.

Udowodniony lemat w połączeniu z twierdzeniem 1 implikuje następującym uogólnieniem owego twierdzenia:

Twierdzenie 1'. *Dla dowolnej liczby całkowitej $n \geq mpq - p - q + 1$ istnieje co najmniej m przedstawień dobrych.*

Zauważmy, że korzystając z lematu 2 i wcześniejszego spostrzeżenia, że liczba $pq - p - q$ nie ma przedstawienia dobrego można wykazać, że liczba $mpq - p - q$ ma $m - 1$ przedstawień dobrych.

Nazwijmy *przewodnikiem dla pary właściwej o danych własnościach* najmniejszą liczbę całkowitą taką, że dla każdej nie mniejszej istnieje właściwa dla niej para liczb a, b lub pewna liczba takich par o danych własnościach. Wykazaliśmy zatem, że przewodnikiem dla istnienia m par właściwych jest liczba $mpq - p - q + 1$.

Rozważę teraz kilka postawionych przeze mnie problemów:

Problem 2. *Czy istnieje przewodnik dla pary właściwej w której jedna z liczb jest kwadratem liczby całkowitej?*

Problem 3. *Czy istnieje przewodnik dla pary właściwej w której jedna z liczb jest pierwsza?*

Problem 4. *Czy istnieje przewodnik dla pary właściwej której liczby kończą się tą samą cyfrą? Ogólniej, czy istnieje przewodnik dla pary właściwej w której liczby dają tą samą resztę z dzielenia przez daną liczbę?*

Twierdzenie 2. *Istnieje przewodnik dla pary właściwej w której jedna z liczb jest kwadratem liczby całkowitej wtedy i tylko wtedy, gdy $p \in \{1, 2\}$ lub $q \in \{1, 2\}$.*

Dowód twierdzenia 2. Załóżmy, że $p = 2$. Wówczas dla każdego danego parzystego n przyjmujemy $a = \frac{n}{2}$, $b = 0$. Wtedy b jest kwadratem liczby całkowitej. Jeśli n jest nieparzysta i większa od q to przyjmujemy $a = \frac{n-q}{2}$, $b = 1$. Wtedy b jest również kwadratem liczby całkowitej. Jeśli natomiast $p = 1$, to wystarczy przyjąć $a = n$, $b = 0$. Przewodnik dla pary w której jedna z liczb jest kwadratem liczby całkowitej i $p = 2$ wynosi $q - 1$ (co łatwo wywnioskować z powyższych rozważań), a dla $p = 1$ wynosi 0. Analogiczny wniosek otrzymamy przy założeniu że $q \in \{1, 2\}$. Załóżmy teraz, że $p \neq 2$, $p \neq 1$ i $q \neq 2$, $q \neq 1$. Udowodnię, iż wtedy istnieją dowolnie duże n które nie mają przedstawienia dobrego w którym jedna z liczb pary właściwej jest kwadratem. Załóżmy więc przeciwnie, że $a = d^2$, gdzie d jest całkowite. Ponieważ $x^2 \equiv (q - x)^2 \pmod{q}$ więc liczba a daje najwyżej $\frac{q}{2} + 1$ różnych reszt z dzielenia przez q . Dla $q > 2$, $\frac{q}{2} + 1 < q$ więc istnieje reszta z dzielenia przez q której a na pewno nie daje. Taka reszta będzie więc też istniała dla liczby ap . Dla dowolnego n dającego właśnie taką resztę z dzielenia przez q równanie $n = ap + bq$ nie będzie miało rozwiązania co kończy dowód.

Możemy zapytać, czy dla pewnych p, q istnieje przewodnik dla pary właściwej której obie liczby są kwadratami liczby całkowitej. Rozumowanie podobne do tego w dowodzie twierdzenia 2 zaprowadzi nas jednak do wniosku, że gdyby istniał, to $p, q \in \{1, 2\}$, co zważając na względną pierwszość tych liczb daje 2 przypadki. Jeśli $p = q = 1$ to przewodnik oczywiście nie istnieje, bo istnieją dowolnie duże liczby nie będące sumą dwóch kwadratów liczb całkowitych. Gdy $p = 1, q = 2$ lub $p = 2, q = 1$ to problem sprowadza się do rozstrzygnięcia czy istnieje liczba taka, że każdą liczbę niemniejszą można przedstawić jako sumę kwadratu liczby całkowitej i dwukrotności kwadratu liczby całkowitej. Taka liczba nie istnieje jednak, gdyż w ten sposób nie można przedstawić na przykład kwadratu liczby parzystej. W przeciwnym wypadku otrzymalibyśmy równość $x^2 + 2y^2 = z^2$ równoważną $z^2 - x^2 = 2y^2$, gdzie z , oraz x są parzyste, skąd po lewej stronie występuje w rozkładzie dwójka z wykładnikiem parzystym (bo to różnica parzystych kwadratów), a po prawej z nieparzystym, co jest sprzeczne.

Twierdzenie 3. *Istnieje przewodnik dla pary właściwej w której jedna z liczb jest pierwsza wtedy i tylko wtedy, gdy jedna z liczb p, q jest pierwsza lub równa 1.*

Dowód twierdzenia 3. Załóżmy, że p jest liczbą pierwszą, oraz dane n jest podzielne przez p . Przyjmujemy $a = \frac{n}{p} - q$, $b = p$, wtedy b jest liczbą pierwszą. Zakładamy oczywiście, że n jest odpowiednio duże, by liczba a była nieujemna. Niech teraz n nie będzie podzielne przez p . Rozważmy pewną liczbę n która daje określoną resztę z dzielenia przez p różną od zera. Zbadajmy ciąg liczb $n, n + p, n + 2p, \dots$. Jeśli $(a, b) = (a_n - kq, b_n + kp)$ dla k dla których liczby tej pary są nieujemne to wszystkie pary właściwe liczby n , to stwierdzamy, że pary właściwe kolejnych wyrazów rozważanego ciągu mają postać $(a, b) = (a_n + l - kq, b_n + kp)$ dla wyrazu $n + lp$, gdzie k jest określone jak wcześniej, oraz l jest oczywiście nieujemne całkowite (robimy to szukając par maksymalnych). Stąd ciąg możliwych liczb b możliwych par właściwych dla danej liczby $n + lp$ jest ciągiem początkowych wyrazów ciągu arytmetycznego o pierwszym wyrazie b_n oraz różnicy p . Liczby te są względnie

pierwsze, bo w przeciwnym wypadku liczba n dzieliłaby się przez ich wspólny dzielnik, który zważając na pierwszość liczby p , wynosiłby właśnie p . To jednak przeczy założeniu.

Korzystając więc z twierdzenia Dirichleta o liczbach pierwszych w ciągu arytmetycznym stwierdzamy, że dla odpowiednio dużych l w ciągu liczb b właściwych dla $n + lp$ będzie występować liczba pierwsza. Z tego już wynika, że jeśli p jest pierwsza to istnieje przewodnik dla pary właściwej w której jedna z liczb jest pierwsza. Jego wartość jest jednak trudna do wyznaczenia. Do analogicznych wniosków dojdziemy przy założeniu, że q jest pierwsza. Niech teraz $p = 1$. Gdy odpowiednio duże n jest postaci rp , gdzie r jest liczbą całkowitą niemniejszą od $2p$, to przyjmujemy $a = 2$, $b = n - 2p$. Analogicznie dla $q = 1$. Gdyby obie liczby p, q były złożone, to przyjmując za n liczbę podzielną przez pq otrzymamy wniosek, że na pewno liczba a z każdej pary właściwej jest podzielna przez q , zaś liczba b z każdej pary właściwej jest podzielna przez p . To kończy dowód.

Zapytajmy teraz podobnie jak wcześniej, czy może istnieje przewodnik dla pary właściwej w której obie liczby są pierwsze lub równe 1. Udowodnię, że nie. Przyjmijmy $n = rpq$ dla pewnego r . Jeśli ta liczba ma przedstawienie dobre $ap + bq$ i liczby a, b są pierwsze, to q dzieli a , zaś p dzieli b . Wtedy $a \in \{1, q\}$, $b \in \{1, p\}$, skąd $\frac{a}{q} \in \{1, \frac{1}{q}\}$, $\frac{b}{p} \in \{1, \frac{1}{p}\}$. Jednak $r = \frac{a}{q} + \frac{b}{p}$ a dowolnie dużą liczbę r możemy wybrać tak, by było nieparzyste i $r - 2$ nie było pierwsze, ani równe 1. Zauważmy, że wtedy równość $r = \frac{a}{q} + \frac{b}{p}$ nie może zachodzić, bo dla takiego r jedna z liczb $\frac{a}{q}, \frac{b}{p}$ musiałaby być równa 2, ale wtedy $r - 2$ nie jest pierwsze ani równe 1.

Twierdzenie 4. *Istnieje przewodnik dla pary właściwej której liczby dają tę samą resztę z dzielenia przez daną liczbę całkowitą dodatnią d wtedy i tylko wtedy, gdy $p + q$ jest względnie pierwsze z d .*

Dowód twierdzenia 4. Wszystkie pary właściwe danej n są postaci $(a, b) = (a_n - kq, b_n + kp)$, więc aby a i b dawały tę samą resztę z dzielenia przez d , $b_n - a_n + k(p + q)$ musi się dzielić przez d . Jeśli $p + q$ jest względnie pierwsze z d , oraz gdy n jest na tyle duże, że k może przyjmować co najmniej d wartości, to korzystając z lematu 1, $k(p + q)$ jest odwrotnością modulo d liczby $b_n - a_n$ dla pewnego k . Dla tej wartości k liczby a, b dają tę samą resztę z dzielenia przez d . Korzystając z twierdzenia 1' szacujemy, że przewodnik dla pary właściwej o tej własności jest nie większy niż $d(p + q) - p - q + 1$. Załóżmy jednak, że $p + q$ i d mają wspólny dzielnik $w > 1$. Jeśli istniałby przewodnik którego wartość to n , to jak stwierdziliśmy $b_n - a_n + k(p + q)$ dzieliłoby się przez d , jak również przez w , skąd $b_n - a_n$ dzieliłoby się przez w . Ponieważ n jest przewodnikiem, więc podobnie jak wcześniej udowadniamy, że $b_{n+1} - a_{n+1}$ dzieli się przez w . Stąd mamy przystawanie $b_{n+1} - b_n \equiv a_{n+1} - a_n \pmod{w}$. W takim wypadku $1 \equiv n + 1 - n \equiv a_{n+1}p + b_{n+1}q - a_np - b_nq \equiv p(a_{n+1} - a_n) + q(b_{n+1} - b_n) \equiv (p + q)(b_{n+1} - b_n) \equiv 0 \pmod{w}$. Jest to sprzeczne, co kończy dowód.

Można by zastanawiać się nad rozszerzeniem definicji przedstawienia dobrego tak, by były dane względnie pierwsze liczby $p_1, p_2, \dots, p_t$, a przedstawieniem dobrym byłoby przedstawienie danej liczby n w postaci $Ap_1 + A_2p_2 + \dots + A_tp_t$, dla pewnych nieujemnych liczb całkowitych $A_1, A_2, \dots, A_t$. Możemy wtedy stawiać problemy analogiczne do tych dla $t = 2$. Wyznaczanie przewodników w tym przypadku jest bardzo trudne, ale samo

dowodzenie ich istnienia niekoniecznie. Wynika to z faktu, że jeśli rozważamy przedstawienia dobre wystarczająco dużych liczb, to możemy wybrać $t - 2$ spośród liczb $A_1, A_2, \dots, A_t$ dowolnie (załóżmy, że $A_3, A_4, \dots, A_t$), a wszystkie możliwe pary pozostałych dwóch liczb są parami właściwymi liczby $n - (A_3p_3 + A_4p_4 + \dots + A_tp_t)$. Rozwiązania problemów związanych z istnieniem przewodników, analogicznych do tych dla $t = 2$, byłyby więc również w pewnym sensie analogiczne do rozwiązań dla $t = 2$.

W naszych rozważaniach ważną rolę odgrywały pary maksymalne. Warto więc przyrzeć się ich strukturze. Udowodnię teraz następujące twierdzenie:

Twierdzenie 5. *Niech dane będzie całkowite $l \geq (p - 1)(q - 1)$. Ciąg $b_l, b_{l+1}, \dots, b_{l+p-1}$ jest permutacją ciągu $0, 1, \dots, p - 1$.*

Dowód twierdzenia 5. Załóżmy, że dla pewnych i, j takich, że $|i - j| \leq p - 1$, $b_i = b_j$. Wtedy jednak $i - j = a_ip + b_iq - a_jp - b_jq = (a_i - a_j)p$. Lewa strona tej równości mieści się w przedziale $< -p + 1, p - 1 >$, zaś prawa jest podzielna przez p , więc musi zachodzić $i - j = 0$ tzn. $i = j$. Stąd wszystkie liczby $b_l, b_{l+1}, \dots, b_{l+p-1}$ są różne. Z drugiej strony wszystkie liczby b_l są mniejsze od p , bo w przeciwnym razie można by zmniejszyć o p liczbę b_l , oraz zwiększyć o q liczbę a_l , co przeczy jej maksymalności. Mamy więc p możliwych wartości $0, 1, \dots, p - 1$ dla każdej z różnych liczb $b_l, b_{l+1}, \dots, b_{l+p-1}$, których jest oczywiście p , skąd już wynika teza.

Zauważmy ponadto, iż $b_i = b_{p+i}$. Jest to konsekwencją tego, iż równości $p = n + p - n = a_{p+i}p + b_{p+i}q - a_ip - b_iq = (a_{p+i} - a_i)p + (b_{p+i} - b_i)q$ będzie wynikało, że $b_{p+i} - b_i$ dzieli się przez p . Zważając na przedział w jakim są zawarte wszystkie b_l , jest to możliwe tylko wtedy, gdy $b_{p+i} = b_i$. Możemy jednak obrać za i inną liczbę. Wyniknie więc z tego, że ciąg b_i dla $i \geq (p - 1)(q - 1)$ jest okresowy o okresie p .

Rozważmy teraz pewien problem:

Problem 5. *Dla danej liczby całkowitej nieujemnej h , wyznaczyć liczbę liczb n , których liczba a pary maksymalnej jest równa h .*

Rozwiązanie. Należy znaleźć liczbę rozwiązań równania $hp = n - b_nq$. Korzystając z wcześniejszego wniosku iż $b_n = b_{n+p}$ stwierdzamy, że $a_np + p = n + p - b_nq = n + p - b_{n+p}q = a_{n+p}p$, czyli $a_n + 1 = a_{n+p}$. Można wyciągnąć z tego bardzo przydatne wnioski. Mianowicie, wśród liczb dających tę samą resztę z dzielenia przez p istnieje najwyżej jedna liczba o liczbie a pary maksymalnej równej h . Stąd liczba rozwiązań rozważanego równania to najwyżej p . Istnieje liczba dająca daną resztę z dzielenia przez p o liczbie a pary maksymalnej równej h wtedy i tylko wtedy, gdy pewna liczba nie większa od h jest liczbą a pewnej pary maksymalnej. Rozważmy liczby $n = (k - lp)q$, dla $k = 0, 1, \dots, p - 1$, oraz l będącego nieujemną liczbą całkowitą dla której wyrażenie $k - lp$ osiąga możliwie najmniejszą wartość nieujemną dla danego k . Na mocy lematu 1 liczby te dają wszystkie możliwe reszty z dzielenia przez p , gdyż przystają do liczby kq modulo p . Z drugiej strony liczba a par maksymalnych tych liczb wynosi zero. W przeciwnym wypadku $bq = n - ap = (k - lp)q - ap$, skąd $q|a$, czyli dla pewnego całkowitego x mamy $n - ap = (k - lp)q - qxp = (k - (l + x)p)q$. Stąd $b = (k - (l + x)p)q$ jest dodatnia, co przeczy minimalności

liczby $k - lp$. Wynika z tego, że istnieje p liczb o liczbie a w parze maksymalnej równej 0 . Ze spostrzeżenia, że $a_n + 1 = a_{n+p}$ wynika, że dla dowolnego h , szukana liczba wynosi p .

Zauważmy też, że jeśli zamiast rozważania ilości liczb o liczbach a pary maksymalnej równych h , rozważać ilości liczb o liczbach a dowolnych par właściwych równych h , to byłoby ich nieskończenie wiele, tzn. $n = hp + ib$, gdzie i jest dowolną liczbą całkowitą nieujemną.

Spróbujmy teraz rozważyć problem związany z ciągami arytmetycznymi:

Problem 6. *Czy istnieje liczba n taka, że wśród liczb a par właściwych liczb kolejno $n, n + 1, n + 2 \dots$ istnieją liczby tworzące nieskończony ciąg arytmetyczny?*

Rozwiązanie. Załóżmy, że takie n istnieje. Niech różnica nieskończonego ciągu wynosi r . Wówczas dla pewnych liczb dodatnich całkowitych a, B_0, B_1 zachodzi równość $n = ap + B_0q$, $n + 1 = (a + r)p + B_1q$ czyli $1 = rp + (B_1 - B_0)q$. Rozważmy teraz pewne liczby $n + i = (a + ri)p + B_iq$, $n + i + 1 = (a + r(i + 1))p + B_{i+1}q$. Wtedy $1 = rp + (B_{i+1} - B_i)q$, skąd $B_1 - B_0 = B_{i+1} - B_i$. Oznacza to że liczby b par właściwych kolejnych liczb różnią się o tę samą liczbę, czyli też tworzą nieskończony ciąg arytmetyczny. Obie liczby $r, B_{i+1} - B_i$ na mocy otrzymanych równości nie mogą być jednak dodatnie, bo w ciągu liczb a lub b w końcu zaczęły by się pojawiać liczby ujemne co jest sprzeczne i oznacza, że jedna z liczb $r, B_{i+1} - B_i$ jest równa zero, a druga jeden, zaś odpowiadająca jej liczba p lub q równa też jeden.

Spróbujmy jednak ulepszyć nasz problem:

Problem 6'. *Czy istnieje taka liczba całkowita dodatnia t , że istnieje taka liczba n , że wśród liczb a par właściwych liczb kolejno $n, n + t, n + 2t, \dots$ istnieją liczby tworzące ciąg arytmetyczny? Jeśli tak, jaka jest najmniejsza liczba t o tej własności? Czy istnieje takie t , że każda liczba niemniejsza ma tę własność?*

Rozwiązanie. Załóżmy, że takie t, n istnieją. Niech różnica nieskończonego ciągu wynosi r . Podobnie jak wcześniej stwierdzamy, że liczby b odpowiednich par właściwych też tworzą ciąg arytmetyczny, którego różnicę oznaczmy przez s . Wówczas rozumując również podobnie jak wcześniej stwierdzamy, że $t = rp + sq$. Stąd łatwo się przekonać, że t ma szukaną własność wtedy i tylko wtedy, gdy posiada przedstawienie dobre. Dowód jest analogiczny jak w rozwiązaniu problemu 6. Najmniejszą liczbą t o zadanych własnościach jest więc $\min(p, q)$, zaś na mocy twierdzenia 1, każda liczba $t \geq (p - 1)(q - 1)$ ma opisywaną własność.

Literatura:

1. Kamila Łyczek - „Kraina dwóch monet” – Delta 4/2014