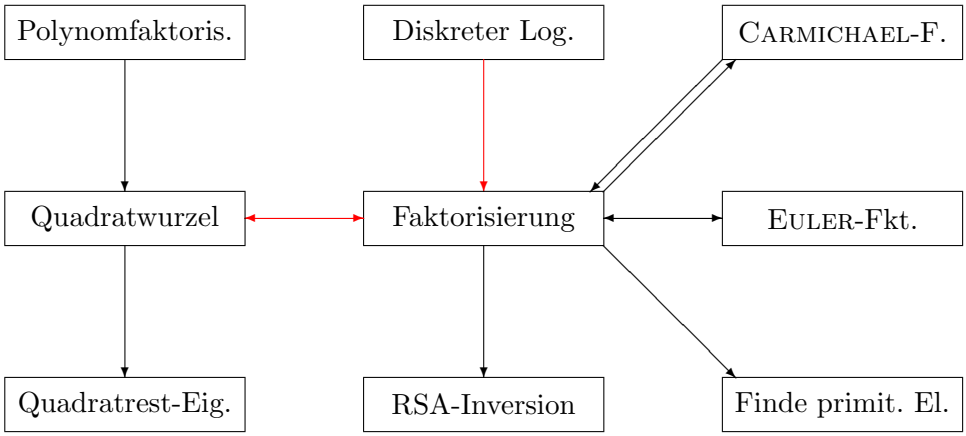
5 Harte zahlentheoretische Probleme

Die folgende Tabelle gibt einen Überblick über kryptologisch relevante zahlentheoretische Berechnungsprobleme. „Effizient“ bedeutet dabei „mit polynomialem Aufwand lösbar“.

Berechnungsproblem	**effizient?**	**behandelt in**
Primzahltest	ja	3.1–3.8
Für Primzahl p		
Finde primitives Element	ja (ERH oder prob.)	A.2, A.10
Finde quadratischen Nichtrest	ja (ERH oder prob.)	A.9
Quadratrest-Eigenschaft	ja	A.6
Quadratwurzel ziehen	ja (ERH oder prob.)	folgt in 5.3
Diskreter Logarithmus	? (vermutlich nein)	4.1, 4.6
Für zusammengesetzte Zahl n		
Faktorisierung	? (vermutlich nein)	2.2, 2.4
RSA-Inversion (e-te Wurzel)	? (vermutlich nein)	2.2
Berechn. der Euler-Funktion	? (vermutlich nein)	2.2
Berechn. der Carmichael-F.	? (vermutlich nein)	2.2
Finde primitives Element	? (vermutlich nein)	A.4
Quadratrest-Eigenschaft	? (vermutlich nein)	A.8
Quadratwurzel ziehen	? (vermutlich nein)	folgt in 5.5
Diskreter Logarithmus	? (vermutlich nein)	folgt in 5.1

„ERH“ bedeutet „unter Annahme der erweiterten Riemannschen Vermutung“, „prob.“ bedeutet „mit einem probabilistischen Algorithmus“.

Der Zusammenhang zwischen den Berechnungsproblemen für eine zusammengesetzte Zahl n wird in der folgenden Grafik dargestellt. Ein Pfeil von A nach B bedeutet dabei, dass das Problem B mit einem effizienten probabilistischen Algorithmus auf das Problem A reduzierbar ist. Die Umkehrungen bei den einfachen Pfeilen sind jeweils unbekannt. Die Reduktionen, die durch rote Pfeile bezeichnet sind, werden im folgenden bewiesen. (Z. T. nur für den Fall, dass n Produkt zweier Primzahlen ist.) [Die mit „Polynomfaktoris.“ bezeichnete Aufgabe, über dem Restklassenring $\mathbb{Z}/n\mathbb{Z}$ Polynome in einer Unbestimmten zu faktorisieren, wird hier nicht weiter behandelt.]


Polynomfaktoris.
Diskreter Log.
Carmichael-F.
Quadratwurzel
Faktorisierung
Euler-Fkt.
Quadratrest-Eig.
RSA-Inversion
Finde primit. El.